Agencia de Protección de Datos
de la Comunidad de Madrid

memoria 2009

Agencia de Protección de Datos
de la Comunidad de Madrid

memoria
2009

Edita: AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID

D.L.: M. XXXX-2010
Imprime: B.O.C.M.
ISSN: 1888-8682

Diseño y maquetación: ARTEGRAF, S.A.

memoria
2009

Índice

Presentación 5

1. Registro de ficheros 7

2. Control de ficheros. Tutela de derechos e inspección 15
   2.1. Procedimientos administrativos 17
      2.1.1. Introducción 17
      2.1.2. Tutela de derechos 17
      2.1.3. Procedimientos de inspección 18
   2.2. Planes de inspección 20
      2.2.1. Introducción 20
      2.2.2. Plan de inspección 2008-2010 sobre el cumplimiento de la normativa de protección de datos en la recogida de los mismos a través de páginas webs de los Ayuntamientos de la Comunidad de Madrid 20

3. Desarrollo normativo 21
   3.1. Introducción 23
   3.2. Instrucción 1/2009, de 17 de diciembre de 2009, sobre el tratamiento de datos personales de los recién nacidos en los centros asistenciales que integran la red sanitaria única de utilización pública de la Comunidad de Madrid (BOCM de 21 de enero de 2010) 23
   3.3. Instrucción 2/2009, de 21 de diciembre de 2009, sobre el tratamiento de datos personales en la emisión de justificantes médicos 24

4. Asesoramiento 25

5. Consultoría 31
   5.1. Planes sectoriales 34
      5.1.1. Videovigilancia 34
      5.1.2. Seguridad 36
         5.1.2.1. Regularización de los niveles de seguridad 36
         5.1.2.2. Auditorías de seguridad 38
      5.1.3. Publicación de datos personales en Internet y boletines oficiales electrónicos 39
      5.1.4. e-Administración en la Comunidad de Madrid 41

6. Día Europeo de Protección de Datos 43

7. Administración Electrónica 49
   7.1. Introducción 51
   7.2. Nuevo portal institucional de la APDCM 51
   7.3. Formación virtual 53
   7.4. CRM (Customer relationship management) 54

ÍNDICE

8. Formación, difusión y gestión del conocimiento 55
   8.1. Jornadas y formación 57
   8.2. Participación de la APDCM en seminarios 60
   8.3. Premios 61
      8.3.1. Premio Europeo a las Mejores Prácticas Públicas en Protección de Datos. V edición 61
      8.3.2. Premio al Mejor Artículo Científico en Protección de Datos 63
   8.4. Formación de alumnos universitarios 63
   8.5. Centro de Investigación y Documentación "Pablo Lucas Murillo de la Cueva" 64

9. Publicaciones 67
   9.1. Seguridad y protección de datos personales 69
   9.2. Revistas 70
      9.2.1. Revista Española de Protección de Datos 70
      9.2.2. Revista digital www.datospersonales.org 71
      9.2.3. Revista digital www.dataprotectionreview.eu 72
   9.3. Monografías de Protección de Datos 74
   9.4. Dípticos sectoriales de información sobre protección de datos 74
   9.5. Transparencia administrativa y protección de datos personales 75
   9.6. Memoria de la V Edición del Premio a las Mejores Prácticas Europeas en materia de Protección de Datos 76

10. Atención al ciudadano 77

11. Colaboración entre la APDCM y otras Autoridades e Instituciones de control 81
   11.1. Grupo de Trabajo entre Agencias 83
      11.1.1. Grupo de Trabajo de Directores 83
      11.1.2. Grupo de Trabajo de Registro de Ficheros 83
      11.1.3. Grupo de Trabajo de Inspección 84
      11.1.4. Grupo de Trabajo de Análisis Jurídico y Normativo 85
   11.2. Convenios y actividad de colaboración 85
      11.2.1. Convenios firmados 85
      11.2.2. Reuniones con otras autoridades de control 86
   11.3. Conferencias del Director en Méjico, Argentina y Uruguay 86

12. Actividad internacional 87
   12.1. 31.ª Conferencia Internacional de Protección de Datos 89
   12.2. EuroPriSe 89
   12.3. Privacy Open Space (PrivacyOS) 90
   12.4. PrimeLife 92
   12.5. Conferencias y Grupos de Trabajo de Autoridades Internacionales de Control 92
      12.5.1. Conferencia de Primavera de Autoridades de Protección de Datos 92
      12.5.2. Grupo de Trabajo de Tratamiento de Quejas de la Unión Europea 93
      12.5.3. Grupo de Trabajo de Telecomunicaciones 93
      12.5.4. VII Encuentro Iberoamericano 93
13. Secretaría General 95

Presentación

Esta memoria recoge las principales actuaciones desarrolladas por la APDCM durante el año 2009 en el marco de un trabajo concienzudo, profesional e intenso, entre las que me gustaría destacar las siguientes:

Como Autoridad de Control, la Agencia ha tramitado 316 expedientes de inspección y tutela de derechos, resaltando, sobre todo, el crecimiento de estos últimos, ya que se ha duplicado su número respecto al año 2008. Asimismo, cada vez son más frecuentes las peticiones de tutela de derechos de cancelación sobre datos personales que aparecen en los Boletines Oficiales.

Siguiendo con la labor inspectora, se han continuado los trabajos iniciados en el año 2008 sobre el cumplimiento del derecho de información en la recogida de datos personales a través de las páginas Webs de los Ayuntamientos de la Comunidad de Madrid.

Por lo que se refiere al Registro de Ficheros de Datos Personales se ha mantenido una tendencia estable en la creación de ficheros, si bien con la aprobación del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, se han realizado tanto supresiones como modificaciones para adaptar los ficheros al contenido de la citada norma.

Con la aprobación de las Instrucciones sobre el tratamiento de datos personales de los recién nacidos en los centros asistenciales que integran la red sanitaria única de utilización pública de la Comunidad de Madrid y sobre el tratamiento de datos personales en la emisión de justificantes médicos, se han adaptado los tratamientos de datos personales en los citados ámbitos a lo dispuesto por la normativa tanto de protección de datos como sectorial.

Por lo que se refiere a la protección de la privacidad de los menores, la APDCM elaboró el *Plan de Comunicación en Protección de Datos Personales para Escolares,* dentro del cual tuvo lugar una sesión informativa en cada uno de los 404 Institutos de Educación Secundaria de la Comunidad de Madrid el 28 de enero de 2009, haciéndolo coincidir con el Día Europeo de la Protección de Datos de Carácter Personal, y que tuvo una gran cobertura en los diferentes medios de comunicación.

Dentro de la labor de consultoría y apoyo al responsable del fichero destaca la realización de diversos planes específicos. Así, en materia de seguridad se ha realizado el requerimiento por parte de la APDCM de las auditorías de los ficheros de nivel medio y básico. Por otra parte, se ha controlado la adecuación de los tratamientos de los responsables de ficheros a la normativa que la APDCM ha aprobado en los últimos años, en

concreto, las instrucciones y recomendaciones relativas a la publicación de datos personales en Internet y Boletines Oficiales electrónicos, tratamiento de datos de carácter personal en servicios de administración electrónica y tratamiento de datos personales a través de videocámaras.

En materia de formación y de promoción de la cultura de protección de datos, se ha editado el manual *Seguridad y protección de datos personales*, siguiendo la línea iniciada en el año 2008 en el que se publicaron diversos manuales sectoriales, y se han consolidado, aun más si cabe, las publicaciones periódicas de la APDCM, www.datospersonales.org, www.dataprotectionreview.eu y la Revista Española de Protección de Datos.

También se han elaborado dípticos sectoriales de protección de datos en materia de salud y servicios sociales, que fueron enviados a los respectivos centros asistenciales para su distribución.

Por otra parte, se realizaron cuatro jornadas específicas, que contaron con la participación no sólo de la APDCM sino también de responsables de ficheros que pudieron exponer su experiencia: IV Jornada de Centros Educativos, II Jornada de Seguridad, II Jornada de Policía Local y Jornada para Equipos de Orientación.

En lo referente al uso de las tecnologías de la información, la APDCM ha cambiado en el año 2009 su portal institucional, con un diseño mucho más atractivo que permite una navegación más fácil dentro del mismo. También se ha diseñado y lanzado, en colaboración con ICM, una herramienta de formación virtual en protección de datos, que ha recibido 1289 solicitudes de empleados públicos para poder realizar este curso on-line.

Por último, no quisiera finalizar sin agradecer la labor y el esfuerzo desarrollado por el personal de la APDCM y mi antecesor en el cargo D. Antonio Troncoso Reigada, sin los cuales la presentación de esta Memoria de actividades sería imposible.

Santiago Abascal Conde
Director de la APDCM

1. Registro de ficheros

1. Registro de ficheros

1. REGISTRO DE FICHEROS

La Ley 8/2001, de 13 de julio, de Protección de Datos de la Comunidad de Madrid, establece en su artículo 18 que la Agencia de Protección de Datos de la Comunidad de Madrid llevará un Registro de Ficheros de Datos de Carácter Personal. Este Registro tiene una doble finalidad: facilitar al ciudadano el ejercicio de sus derechos, respecto a los tratamientos de datos realizados por las instituciones públicas del ámbito territorial de la Comunidad de Madrid, y servir de medio instrumental para el cumplimiento de sus funciones al resto de unidades y órganos de la Agencia.

Serán objeto de inscripción en el Registro de Ficheros de Datos Personales: los ficheros de datos de carácter personal que sean titulares Instituciones de la Comunidad de Madrid y por los Órganos, Organismos, Entidades de Derecho público y demás Entes públicos integrantes de su Administración Pública, exceptuándose las sociedades mercantiles. También deberán inscribir los ficheros de datos de carácter personal que sean creados o gestionados por los Entes que integran la Administración Local del ámbito territorial de la Comunidad de Madrid, de conformidad con lo previsto en el artículo 41 de la Ley Orgánica 15/1999, de 13 de diciembre, así como sobre los ficheros creados o gestionados por las Universidades Públicas y por las Corporaciones de Derecho público representativas de intereses económicos y profesionales de la Comunidad de Madrid, en este último caso siempre y cuando dichos ficheros sean creados o gestionados para el ejercicio de potestades de derecho público.

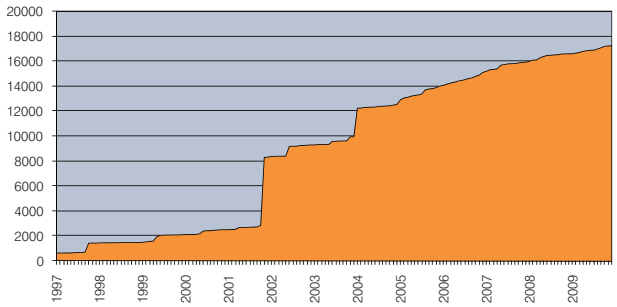
La consulta al Registro de Ficheros es gratuita y está disponible para cualquier persona que lo solicite, especialmente a través de Internet en el sitio web de la Agencia, *www.apdcm.es*, canal “Registro de Ficheros”.

Tal como establece el artículo 20.2 de la Ley 8/2001, periódicamente, la Agencia de Protección de Datos de la Comunidad de Madrid remitirá a la Agencia Española de Protección de Datos el contenido del Registro de Ficheros de Datos Personales de la Comunidad de Madrid, al objeto de su inscripción en el Registro General de Protección de Datos.

Las inscripciones de nuevos ficheros realizadas durante el año 2009 mantienen una tendencia estable de crecimiento respecto a años anteriores. La motivación de esta situación debe buscarse en el alto nivel de regularización de ficheros ya existente en determinados ámbitos de competencia de la Agencia de Protección de Datos de la Comunidad de Madrid, especialmente en su Administración, el haberse alcanzado desde el año 2007 el 100% de Colegios Profesionales con ficheros declarados y, en el primer semestre de 2008, el 100% de Ayuntamientos del ámbito territorial de la Comunidad de Madrid con ficheros inscritos en el Registro. Este incremento también viene motivado por el creciente número de ficheros de videovigilancia, ya que la APDCM está trabajando con los responsables de ficheros para regularizarlos.

1. REGISTRO DE FICHEROS

Evolución cronológica de TOTAL Ficheros Registrados



Asimismo, durante el año 2009 ha habido un aumento de supresión de ficheros que viene justificado por la aplicación del artículo 2.2 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, en virtud del cual el citado Reglamento no se aplica a los tratamientos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

Debe destacarse que no se contabilizan en los diferentes cuadros las modificaciones de las inscripciones que se han realizado como consecuencia de los cambios en la estructura orgánica de las diferentes Consejerías que forman la Administración de la Comunidad de Madrid. Esta tarea de adecuación de las inscripciones, que sólo se realiza de forma periódica en la Comunidad de Madrid, alcanza una media de 8000 inscripciones de modificación por cada cambio de estructura realizada.

En este sentido, estas modificaciones se realizan de oficio por la APDCM de conformidad con lo dispuesto en la Disposición Adicional Primera del Decreto 99/2002, de 13 de junio, que regula el procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro de Ficheros de Datos Personal, siendo el propio decreto de estructura aprobado la disposición de carácter general que habilita para realizar las oportunas modificaciones en el citado Registro.

La adecuación de las inscripciones de ficheros a la nueva estructura de Consejerías permite a los ciudadanos una forma efectiva de identificación de la

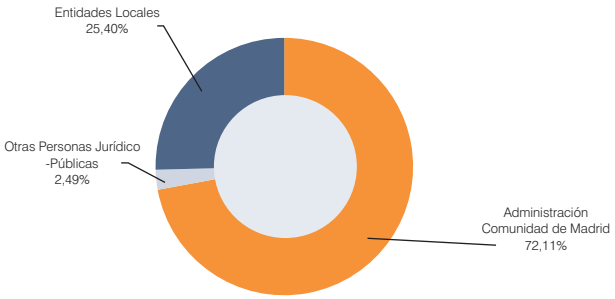
INDICADOR	FICHEROS REGISTRADOS (SOLO ACTIVOS)						
	2005	2006	2007	2008	2009	Variación	
Administración Comunidad de Madrid	11.311	11.390	11.727	11.959	9.905	-2.054	-17,18%
Otras Personas Jurídico - Públicas	237	278	310	323	342	19	5,88%
Entidades Locales	1.621	2.530	2.884	3.244	3.489	245	7,55%
TOTAL	**13.169**	**14.198**	**14.921**	**15.526**	**13.736**	**-1.790**	**-11,53%**

INDICADOR	FICHEROS REGISTRADOS (INCLUIDAS SUPRESIONES Y PROVISIONALES)						
	2005	2006	2007	2008	2009	Variación	
Administración Comunidad de Madrid	11.311	11.982	12.508	12.792	12.988	196	1,53%
Otras Personas Jurídico - Públicas	237	288	326	350	379	29	8,29%
Entidades Locales	1.621	2.691	3.088	3.498	3.881	383	10,95%
TOTAL	**13.169**	**14.961**	**15.922**	**16.640**	**17.248**	**608**	**3,82%**

titularidad de los tratamientos de datos que se realizan en el ámbito de la Administración de la Comunidad de Madrid y, sobre todo, les permite el ejercicio de los derechos que la normativa de protección de datos establece ante el órgano en quien realmente reside la competencia para el tratamiento de sus datos.

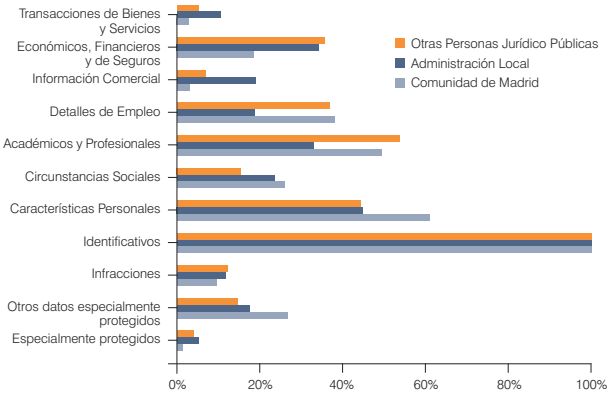
Otro importante número de inscripciones de modificación de ficheros (más de 4000) se han realizado para la adecuación del nivel de seguridad inscrito, en aquellos ficheros creados como manuales, a los que se les han aplicado las especificaciones contenidas en el Real Decreto 1720/2007, de 21 de diciembre.

Ficheros Inscritos por Tipo Administración (31/12/2009)



En cuanto a la clasificación del Registro de Ficheros en función del tipo de datos, a parte de los datos de carácter identificativos que deben contener todos los ficheros, se observa que la mayor parte corresponde a los ficheros con datos académicos y profesionales, así como de características personales.

Promedio de Ficheros Registrados según tipo de Datos



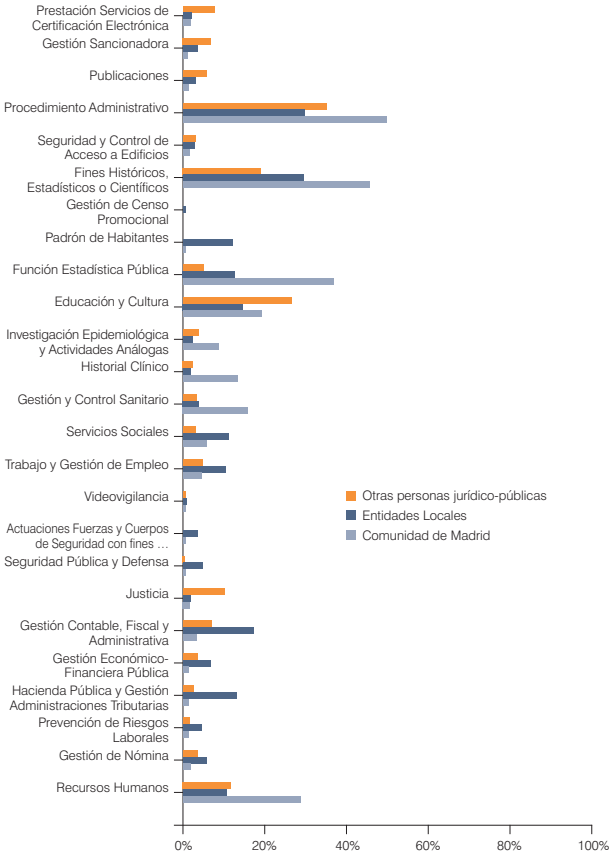
Por lo que respecta a la finalidad, al ser las Administraciones Públicas prestadoras de servicios públicos casi el 50% de los ficheros inscritos tienen como finalidad la tramitación de procedimientos administrativos.

FICHEROS REGISTRADOS SEGÚN TIPO DE DATOS	COMUNIDAD MADRID		ENTIDADES LOCALES		OTRAS PERSONAS JURÍDICO-PÚBLICAS		TOTAL	
	Ficheros	%	Ficheros	%	Ficheros	%	Ficheros	%
Especialmente protegidos	168	1,29%	202	5,20%	15	3,96%	**385**	**2,23%**
Otros datos especialmente protegidos	3.460	26,64%	673	17,34%	55	14,51%	**4.188**	**24,28%**
Infracciones	1.232	9,49%	452	11,65%	46	12,14%	**1.730**	**10,03%**
Identificativos	12.988	100,00%	3.881	100,00%	379	100,00%	**17.248**	**100,00%**
Características personales	7.939	61,13%	1.741	44,86%	168	44,33%	**9.848**	**57,10%**
Circunstancias sociales	3.394	26,13%	911	23,47%	58	15,30%	**4.363**	**25,30%**
Académicos y profesionales	6.390	49,20%	1.273	32,80%	204	53,83%	**7.867**	**45,61%**
Detalles de empleo	4.935	38,00%	718	18,50%	139	36,68%	**5.792**	**33,58%**
Información comercial	399	3,07%	731	18,84%	25	6,60%	**1.155**	**6,70%**
Económicos, financieros y de seguros	2.374	18,28%	1.328	34,22%	135	35,62%	**3.837**	**22,25%**
Transacciones de bienes y servicios	371	2,86%	400	10,31%	19	5,01%	**790**	**4,58%**

1. REGISTRO DE FICHEROS

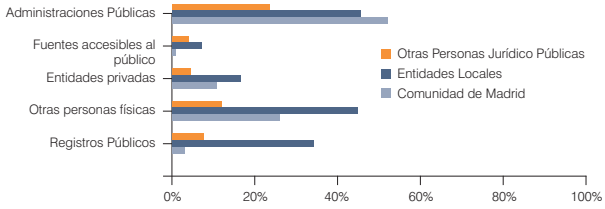
FICHEROS REGISTRADOS SEGÚN FINALIDAD	COMUNIDAD MADRID		ENTIDADES LOCALES		OTRAS PERSONAS JURÍDICO-PÚBLICAS		TOTAL	
	Ficheros	%	Ficheros	%	Ficheros	%	Ficheros	%
Recursos Humanos	3.685	28,37%	408	10,51%	44	11,61%	**4.137**	**23,99%**
Gestión de Nómina	199	1,53%	206	5,31%	12	3,17%	**417**	**2,42%**
Prevención de Riesgos Laborales	101	0,78%	156	4,02%	5	1,32%	**262**	**1,52%**
Hacienda Pública y Gestión Administraciones Tributarias	133	1,02%	500	12,88%	9	2,37%	**642**	**3,72%**
Gestión Económico-Financiera Pública	131	1,01%	244	6,29%	12	3,17%	**387**	**2,24%**
Gestión Contable, Fiscal y Administrativa	394	3,03%	661	17,03%	25	6,60%	**1.080**	**6,26%**
Justicia	192	1,48%	56	1,44%	37	9,76%	**285**	**1,65%**
Seguridad Pública y Defensa	29	0,22%	169	4,35%	1	0,26%	**199**	**1,15%**
Actuaciones Fuerzas y Cuerpos de Seguridad con fines policiales	12	0,09%	123	3,17%	0	0,00%	**135**	**0,78%**
Videovigilancia	33	0,25%	12	0,31%	1	0,26%	**46**	**0,27%**
Trabajo y Gestión de Empleo	521	4,01%	386	9,95%	17	4,49%	**924**	**5,36%**
Servicios Sociales	681	5,24%	420	10,82%	10	2,64%	**1.111**	**6,44%**
Gestión y control sanitario	2.025	15,59%	141	3,63%	11	2,90%	**2.177**	**12,62%**
Historial clínico	1.680	12,94%	63	1,62%	8	2,11%	**1.751**	**10,15%**
Investigación Epidemiológica y actividades análogas	1.109	8,54%	73	1,88%	13	3,43%	**1.195**	**6,93%**
Educación y Cultura	2.437	18,76%	558	14,38%	100	26,39%	**3.095**	**17,94%**
Función Estadística Pública	4.780	36,80%	483	12,45%	17	4,49%	**5.280**	**30,61%**
Padrón de Habitantes	32	0,25%	454	11,70%	0	0,00%	**486**	**2,82%**
Gestión de Censo Promocional	0	0,00%	6	0,15%	0	0,00%	**6**	**0,03%**
Fines Históricos, Estadísticos o Científicos	5.880	45,27%	1.126	29,01%	71	18,73%	**7.077**	**41,03%**
Seguridad y control de acceso a edificios	163	1,26%	47	1,21%	10	2,64%	**220**	**1,28%**
Procedimiento Administrativo	6.438	49,57%	1.143	29,45%	132	34,83%	**7.713**	**44,72%**
Publicaciones	130	1,00%	51	1,31%	20	5,28%	**201**	**1,17%**
Gestión sancionadora	117	0,90%	125	3,22%	25	6,60%	**267**	**1,55%**
Prestación Servicios de Certificación Electrónica	188	1,45%	68	1,75%	28	7,39%	**284**	**1,65%**

Promedio de Ficheros Registrados según Finalidad



Por último, en cuanto a la procedencia de los datos, teniendo en cuenta la misma justificación que en la estadística anterior, más del 50% proceden de las citadas Administraciones Públicas.

Promedio de Ficheros Registrados según Procedencia de los Datos



FICHEROS REGISTRADOS SEGÚN PROCEDENCIA DE LOS DATOS	COMUNIDAD MADRID		ENTIDADES LOCALES		OTRAS PERSONAS JURÍDICO-PÚBLICAS		TOTAL	
	Ficheros	%	Ficheros	%	Ficheros	%	Ficheros	%
Registros Públicos	406	3,13%	1.322	34,06%	30	7,92%	**1.758**	**10,19%**
Otras personas físicas	3.386	26,07%	1.739	44,81%	46	12,14%	**5.171**	**29,98%**
Entidades Privadas	1.421	10,94%	650	16,75%	17	4,49%	**2.088**	**12,11%**
Fuentes Accesibles al Público	124	0,95%	282	7,27%	16	4,22%	**422**	**2,45%**
Administraciones Públicas	6.762	52,06%	1.768	45,56%	89	23,48%	**8.619**	**49,97%**

2. Control de Ficheros. Tutela de Derechos e Inspección

2. Control de Ficheros. Tutela de Derechos e Inspección

2. CONTROL DE FICHEROS. TUTELA DE DERECHOS E INSPECCIÓN

2.1. PROCEDIMIENTOS ADMINISTRATIVOS

2.1.1. Introducción

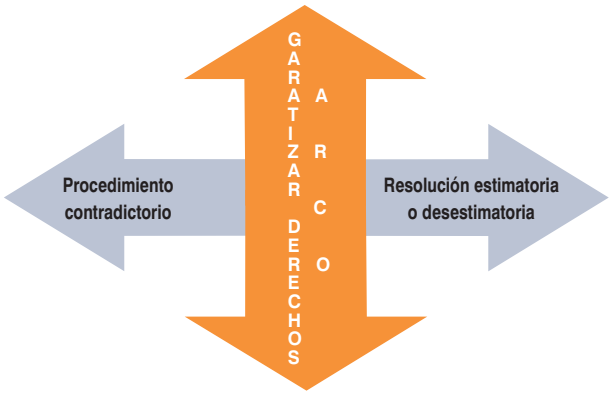
La Subdirección de Inspección y Tutela de Derechos es la unidad administrativa de la APDCM a la que compete el ejercicio de las funciones derivadas de la potestad de inspección, reguladas en el artículo 19 de la Ley 8/2001, de 13 de julio.

En este sentido, es competencia de esta unidad administrativa el impulso y la instrucción de los procedimientos a que den lugar las reclamaciones y denuncias de los ciudadanos para la protección de sus derechos de acceso, rectificación, cancelación y oposición, así como de los procedimientos de infracción de las Administraciones Públicas que se tramiten como consecuencia del ejercicio de la función de control para determinar la existencia o no de una infracción prevista en la LOPD.

2.1.2. Tutela de derechos

El procedimiento administrativo de tutela de derechos se inicia siempre mediante una reclamación interpuesta por el ciudadano cuando éste considera que el responsable del fichero no ha atendido correctamente sus derechos de acceso, rectificación, cancelación y oposición.

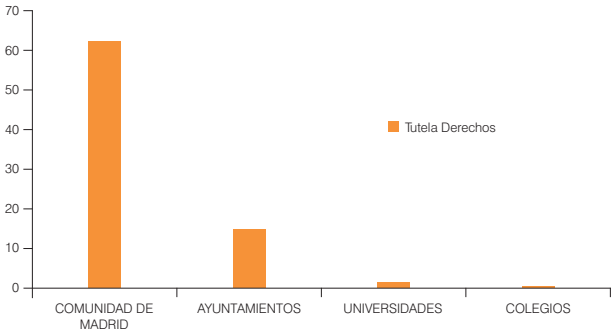
Este procedimiento se encuentra regulado en el Decreto 67/2003, de 22 de mayo. Dicho procedimiento se caracteriza por su carácter contradictorio, de manera que tanto el ciudadano como el responsable del fichero pueden presentar alegaciones para su defensa. La resolución de la APDCM será estimatoria si considera que el derecho de acceso, rectificación, oposición o cancelación no ha sido debidamente atendido o desestimatoria en caso contrario.



Al igual que en años anteriores, se ha experimentado un crecimiento continuo de los procedimientos de tutela de derechos. Así, si durante 2008 se interpusieron 54 reclamaciones sobre el ejercicio de los derechos ARCO, en 2009 casi se ha duplicado este número, con un total de 101 reclamaciones.

Este progresivo aumento está motivado por dos circunstancias: en primer lugar, las Autoridades de Control de Protección de Datos, incluyendo, como es obvio, a la APDCM, están tutelando el ejercicio de los derechos ARCO respecto a las historias clínicas. En este sentido, durante el 2009 se recibieron 25 re-

clamaciones de los ciudadanos sobre el ejercicio de los derechos ARCO respecto a los ficheros obrantes en la Consejería de Sanidad, siendo la mayor parte de ellos solicitudes de acceso o cancelación a la historia clínica. En segundo lugar, cada vez son más frecuentes las reclamaciones planteadas que solicitan la tutela del derecho de cancelación en relación a los datos publicados en boletines o diarios oficiales.



2.1.3. Procedimientos de inspección

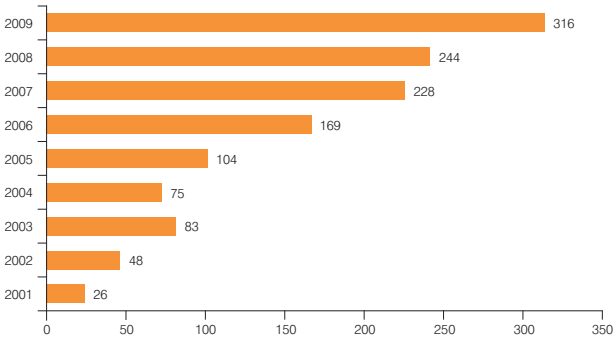
El procedimiento de inspección se inicia siempre de oficio, si bien la mayoría de las veces el citado inicio viene motivado por la presentación de una denuncia por parte del ciudadano. Asimismo, la APDCM también abre este tipo de procedimientos de oficio por otras vías: bien cuando inicia un plan de inspección, bien cuando aparece alguna noticia en prensa de la que puede derivar una infracción en materia de protección de datos, bien cuando se tiene constancia por otros medios de que puede producirse un incumplimiento de la normativa de protección de datos.

Al igual que el procedimiento de tutela de derechos, el procedimiento de inspección se encuentra establecido en el Decreto 67/2002, de 22 de mayo. Este Decreto regula, además de la inspección propiamente dicha, el procedimiento de infracción en el supuesto de que en las actuaciones realizadas existan indicios

de que se ha vulnerado, por parte del responsable del fichero, la protección de datos.

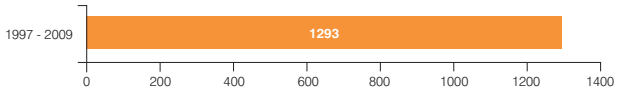
Si en la Memoria del año 2008 ya hacíamos alusión a un ostensible crecimiento del número de expedientes de inspección, incluyendo los de tutela de derechos, desde el año 2001, en el año 2009 se han abierto un total de 316 procedimientos de inspección. A diferencia del año 2008, en el que el aumento de expedientes venía motivado, en gran medida, a los planes de inspecciones ejecutados por la APDCM, en el ejercicio 2009 ha sido, esencialmente, la interposición de reclamaciones por los ciudadanos la que ha hecho que el citado número aumente.

Expedientes tramitados
Función de control y tutela de derechos



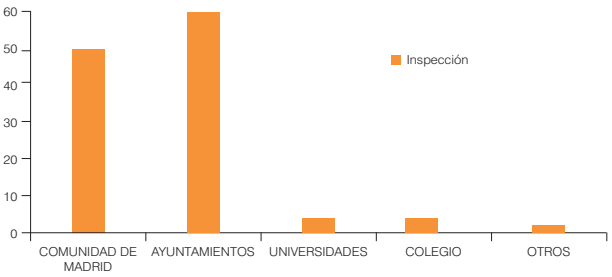
En este sentido, es necesario resaltar que desde la creación de la APDCM ya se han tramitado más un millar de expedientes de inspección y de tutela de derechos.

Expedientes tramitados
Función de control y tutela de derecho

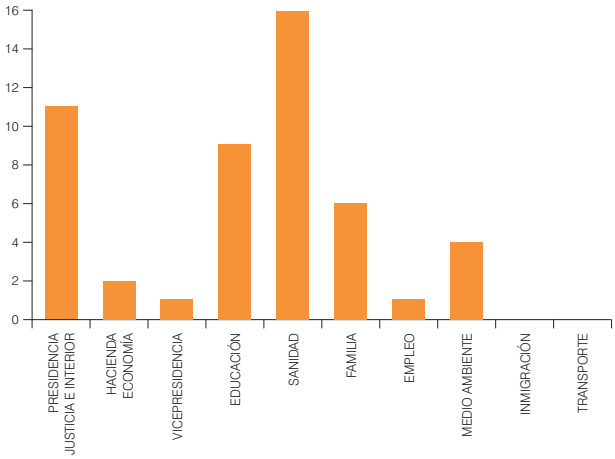


De los 316 expedientes tramitados, tenemos que distinguir entre los que se corresponden con la función inspectora y los que se corresponden con la función de tutela de derechos.

Respecto a los primeros, se han tramitado 215 procedimientos, correspondiendo cincuenta a la Administración de la Comunidad de Madrid, sesenta a la Administración Local, cuatro a las Universidades, cuatro a las Corporaciones de Derecho público y dos a otras Instituciones Públicas. Además, 62 eran competencia de la Agencia Española de Protección de Datos.



En relación a los expedientes de inspección que se han tramitado contra los órganos de la Comunidad de Madrid, dieciséis correspondieron a la Consejería de Sanidad, nueve a la Consejería de Educación, once a la Consejería de Presidencia, Justicia e Interior, seis a la Consejería de Familia y Asuntos Sociales, cuatro a la Consejería de Medio Ambiente, Vivienda y Ordenación del Territorio, dos a la Consejería de Economía y Hacienda, uno a la Consejería de Empleo y Mujer y otro a la Vicepresidencia, Consejería de Cultura y Deportes y Portavocía del Gobierno.



En 2009 se han dictado trece resoluciones —en el año 2008 se dictaron ocho— de infracción debido al incumplimiento por parte del responsable del fichero de alguno de los principios de la LOPD. Entre éstas, podemos citar las siguientes:

- Resolución de infracción a un Centro de Salud por ausencia de medidas de seguridad.
- Resolución de infracción por vulneración del principio de calidad de un Ayuntamiento en el uso de la firma digital.
- Resolución de infracción a un Ayuntamiento por no tener los datos de un ciudadano debidamente actualizados.
- Resolución de infracción a un Centro de Salud por ceder datos personales sin que existiera consentimiento o se diesen alguna de las circunstancias del art. 11.2 de la LOPD.

Por último, la APDCM publica las resoluciones de sus procedimientos tanto de inspección como de tutela de derechos, debidamente anonimizadas, en su página web institucional *(www.apdcm.es)*, dando cumplimiento de esta forma al principio de transparencia administrativa.

2.2. PLANES DE INSPECCIÓN

2.2.1. Introducción

El artículo 18 del Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de las funciones de la APDCM de tutela de derechos y control de ficheros de datos de carácter personal, regula los Planes Sectoriales de Inspección, como una de las manifestaciones de la función de control de la APDCM.

Estos Planes, de carácter preventivo, consisten en analizar por cada uno de los sectores de la actividad administrativa pública, cuyos ficheros se encuentran bajo el ámbito de aplicación de la Ley 8/2001, de 13 de julio, cuál es el grado de adecuación y cumplimiento que dichos ficheros tienen a los principios de la protección de datos, intentando garantizar que los responsables de los ficheros públicos hagan efectivo el cumplimiento de los derechos de acceso, rectificación, cancelación y oposición que ejercen los ciudadanos.

Una vez analizada por los inspectores toda la información y concluidas las actuaciones y comprobaciones necesarias, el Director de la APDCM dicta, de conformidad con el artículo 15.d) de la Ley 8/2001, de 13 de julio, las instrucciones precisas, en las que se determina si los ficheros públicos objeto del plan sectorial están adecuados o no a la normativa de protección de datos.

2.2.2. Plan de inspección 2008-2010 sobre el cumplimiento de la normativa de protección de datos en la recogida de los mismos a través de páginas webs de los Ayuntamientos de la Comunidad de Madrid

En 2008 la APDCM puso en marcha este Plan de Inspección para conocer el grado de cumplimiento de la Recomendación 3/2008, de 30 de abril, de la APDCM, sobre tratamiento de datos de carácter personal en los servicios de Administración Electrónica (ver apartado 3.4 de la Memoria del año 2008).

En el ámbito de la Administración Local y en reconocimiento del derecho de los ciudadanos a relacionarse con la Administración por medios electrónicos (Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos), numerosos Ayuntamientos del territorio de la Comunidad de Madrid, aprovechando el empuje de las tecnologías, han puesto en servicio diferentes páginas webs para que el ciudadano pueda realizar sus trámites administrativos.

Si bien este Plan de Inspección se diseñó para ser ejecutado en el periodo 2008-2009, tras la aprobación de diversas normas reglamentarias que desarrollan la citada Ley, la APDCM consideró conveniente ampliar el plazo de ejecución del mismo hasta el año 2010.

En este sentido, y como indicamos en la Memoria del año 2008 (ver su apartado 2.2.2), una vez que se hayan realizado todas las actuaciones de investigación, se procederá a enviar una Instrucción singular a cada Ayuntamiento para que adecue la recogida de datos personales a través de la página web correspondiente a la normativa de protección de datos y, especialmente, a lo dispuesto en el artículo 5 de la LOPD, así como una Instrucción general dirigida a todos los Ayuntamientos, tanto a los que han sido inspeccionados como a los que no, y que pueda resultar de utilidad para el resto de responsables de ficheros sobre los que la APDCM ejerce su función de control.

3. Desarrollo normativo

3. Desarrollo normativo

3. DESARROLLO NORMATIVO

3.1. INTRODUCCIÓN

El artículo 6 del Decreto 40/2004, de 18 de marzo, por el que se aprueba el Estatuto de la APDCM, regula el desarrollo normativo, de manera que la APDCM puede dictar instrucciones y recomendaciones dentro de su ámbito competencial para adecuar los tratamientos de datos de carácter personal a los principios de la legislación vigente en materia de protección de datos.

En este sentido, siguiendo la línea iniciada hace varios años y que motivó la aprobación en 2008 de la Recomendación 1/2008, de 14 de abril, sobre el tratamiento de datos personales en los Servicios Sociales de la Administración de la Comunidad de Madrid y en los Servicios Sociales de los Entes Locales de la Comunidad de Madrid (*BOCM* de 7 de mayo de 2008), la Recomendación 2/2008, de 25 de abril, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios webs institucionales y en otros medios electrónicos y telemáticos (*BOCM* de 8 de septiembre de 2008), y la Recomendación 3/2008, de 25 de abril, sobre tratamiento de datos de carácter personal en servicios de administración electrónica (*BOCM* de 11 de septiembre de 2008), en el año 2009 la APDCM ha aprobado dos nuevas instrucciones, dirigidas, sobre todo, a los responsables de ficheros del ámbito sanitario.

3.2. INSTRUCCIÓN 1/2009, DE 17 DE DICIEMBRE DE 2009, SOBRE EL TRATAMIENTO DE DATOS PERSONALES DE LOS RECIÉN NACIDOS EN LOS CENTROS ASISTENCIALES QUE INTEGRAN LA RED SANITARIA ÚNICA DE UTILIZACIÓN PÚBLICA DE LA COMUNIDAD DE MADRID (BOCM DE 21 DE ENERO DE 2010)

La finalidad principal de la Instrucción relativa a la identificación de los recién nacidos es mejorar los procedimientos de toma de huellas, tanto del recién nacido como de la madre, permitiendo realizar una identificación y vinculación inequívoca de ambos, evitando confusiones y problemas de intercambio de bebés en los centros asistenciales. La incorrecta identificación de los recién nacidos deja sin sentido la existencia de una tarjeta de identificación sanitaria, al tiempo que impide su correcta inscripción en el Registro Civil.

La recogida de las huellas dactilares constituye el sistema que permite una identificación inequívoca de ambos, así como para establecer la correspondencia entre el recién nacido y su madre biológica. Tal y como establece la Ley 6/1995, de 28 de marzo, de Garantías de los Derechos de la Infancia y la Adolescencia en la Comunidad de Madrid, deberán utilizarse para la toma de los datos los métodos más avanzados y precisos disponibles, evitando que los posibles defectos en la toma de las huellas

hagan que el Documento de Identificación carezca de utilidad.

Dada la finalidad para la que se recogen los datos, éstos no podrán ser objeto de cancelación, al seguir siendo necesarios y pertinentes durante toda la vida del recién nacido y de la madre. Si los datos recogidos en el Documento de Identificación Sanitaria Materno-Filial fueran conservados dentro de la historia clínica, éstos no podrán ser objeto de expurgo ni cancelación, aun transcurridos los plazos de conservación para la historia clínica que se establecen en la Ley 41/2002, de 14 de noviembre, Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y Documentación Clínica.

3.3. Instrucción 2/2009, de 21 de diciembre de 2009, sobre el tratamiento de datos personales en la emisión de justificantes médicos. (BOCM de 21 de enero de 2010)

Esta Instrucción incide en la necesidad de que no se faciliten a los departamentos de personal más datos de los que realmente son necesarios para justificar una ausencia al trabajo, evitando que se pueda conocer el diagnóstico o causa concreta de la enfermedad del trabajador, tal como ya recoge la normativa que regula la emisión de los partes de baja.

Si bien no es necesario presentar en los casos de ausencia al trabajo por enfermedad común o accidente no laboral el parte de baja, el trabajador tiene que justificar la ausencia al trabajo, por lo que los centros sanitarios deben facilitar al paciente un documento que acredite la asistencia o servicio prestado.

Un aspecto concreto regulado en esta Instrucción es la diferenciación de los supuestos en que el solicitante del justificante es el propio trabajador enfermo o cualquier persona que tenga con él una relación familiar o de hecho, requiriéndose en este último caso el consentimiento inequívoco del enfermo o usuario del centro sanitario.

Además, deben diseñarse procedimientos específicos para este tratamiento de datos, evitando utilizar documentos creados para la gestión asistencial —como son la propia hoja de citación— como justificante, dado que en ésta se hace mención al posible problema de salud que pueda existir o a la prueba diagnóstica a la que haya sido sometido el paciente.

4. Asesoramiento

4. Asesoramiento

4. ASESORAMIENTO

Dentro de la actividad de asesoramiento llevada a cabo mediante la realización de informes, podemos distinguir cuatro tipos:

- Informes preceptivos sobre la creación, modificación y supresión de ficheros.
- Informes sobre la adaptación de contratos y convenios al artículo 12 de la LOPD (encargados del tratamiento).
- Informes preceptivos a la aprobación de normas.
- Informes que dan respuesta a las consultas planteadas por los responsables de ficheros.

En lo que se refiere a los primeros, se trata de una obligación que establece la Ley 8/2001, de 13 de julio, de Protección de Datos Personales en la Comunidad de Madrid, ya que, con carácter previo a la aprobación de la disposición de carácter general de creación, modificación o supresión de un fichero, el proyecto, junto con las alegaciones, se debe enviar a la APDCM para su informe preceptivo. A través del citado informe, y analizando previamente toda la documentación enviada, la APDCM ejerce una actividad de *prior checking*, es decir, un control previo de legalidad sobre el tratamiento de datos personales que se pretenda realizar. Así, en el año 2009, se han elaborado 145 informes preceptivos de este tipo.

INDICADOR	2007	2008	2009
Disposiciones generales de ficheros publicadas	121	160	136
Ficheros regulados por disposiciones publicadas	1.150	828	6.906

Respecto a los informes sobre la adaptación de contratos y convenios al artículo 12 de la LOPD (encargados del tratamiento), según este artículo cuando se realice un tratamiento por cuenta de terceros debe existir un contrato o convenio en el cual se estipulen las obligaciones que debe cumplir el encargado del tratamiento respecto a los datos personales.

En este sentido, y con carácter previo a su firma o perfeccionamiento, la APDCM ha informado 143 (en el año 2008 fueron 132) convenios y contratos en relación a su adecuación al artículo 12 de la LOPD.

INFORMES SOBRE CONTRATOS Y CONVENIOS DEL ARTÍCULO 12 DE LA LOPD	
Vicepresidencia, Consejería de Cultura y Deportes y Portavocía del Gobierno	3
Consejería de Presidencia, Justicia e Interior	24
Consejería de Economía y Hacienda	7
Consejería de Medio Ambiente y Ordenación del Territorio	1
Consejería de Sanidad	48
Consejería de Familia y Asuntos Sociales	4
Consejería de Empleo y Mujer	34
Entes Locales	21
Universidades	1
TOTAL	**143**

4. ASESORAMIENTO

En referencia a los informes preceptivos a la aprobación de normas, la APDCM ha informado preceptivamente, en fase de proyecto, durante el año 2009 un total de 210 normas, lo que supone un incremento del 53% con respecto al año 2008, en el que se informaron 137 normas. Entre ellas, destacan las siguientes:

- Decreto por el que se autoriza a Madrid Movilidad, S. A. el uso de medios de captación remota, a través de fotografías, filmación digital y otros medios tecnológicos, para su traslado a los agentes de la autoridad.
- Decreto del Consejo de Gobierno de la Comunidad de Madrid por el que se regula el procedimiento para el nombramiento de personal emérito en el Servicio Madrileño de Salud.
- Real Decreto por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud.
- Dictamen de la Comisión de Asuntos Constitucionales y Gobernanza Europea y Espacio de Libertad, Seguridad y Justicia del Comité de las Regiones, "El programa de Estocolmo: retos y oportunidades para un nuevo programa multianual para el espacio de Libertad, Seguridad y Justicia de la Unión Europea".
- Decreto de Consejo de Gobierno por el que se regula el procedimiento para el ejercicio de la libertad de elección de médico de familia, pediatra y enfermero en atención primaria y de hospital y de médico en atención especializada.
- Decreto del Consejo de Gobierno de la Comunidad de Madrid por el que se regula la edición electrónica del *Boletín Oficial de la Comunidad de Madrid*.
- Decreto de simplificación del procedimiento de autorización y registro de Centros, Servicios y Establecimientos Sanitarios de la Comunidad de Madrid.

Asimismo, tal y como se viene desarrollando desde hace años, la APDCM también ha informado sobre numerosas convocatorias de subvenciones, entre las que podemos destacar las siguientes:

- Orden por la que se establecen las bases reguladoras para la concesión de la ayuda económica de pago único, por nacimiento o adopción de tercer o sucesivos hijos, a las familias de la Comunidad de Madrid y se aprueba la convocatoria para 2009.
- Orden por la que se aprueban las bases reguladoras para el fomento de la innovación tecnológica en el sector de la automoción de la Comunidad de Madrid y se convocan ayudas para el año 2009.
- Orden por la que se crea el Fondo Económico de Emergencia para Víctimas de Violencia de Género de la Comunidad de Madrid y se regulan las ayudas con cargo a dicho fondo.
- Acuerdo del Consejo de Gobierno "por el que se aprueban las normas reguladoras y se desarrolla el procedimiento de concesión directa de ayudas económicas de pago único a las familias de la Comunidad de Madrid".
- Orden por la que se aprueban las bases reguladoras y se convocan subvenciones destinadas a municipios de la Comunidad de Madrid, para la prestación de Servicios de Bolsas de Vivienda Joven en Alquiler e Hipoteca Joven.

Por último, respecto a los informes que dan respuesta a las consultas planteadas por los responsables de ficheros, a través de los mismos se da respuesta a las mismas. Estas consultas versan sobre cuestio-

nes relativas a cesiones de datos personales y a la adecuación de tratamientos de datos personales a la LOPD. Mientras en el año 2008 se respondieron a un total de 73 consultas planteadas por los citados responsables, en el año 2009 se han respondido 98, suponiendo un incremento del 34%.

Las consultas más destacadas en 2009 a las que la APDCM ha dado respuesta son las siguientes:

- Entrega a una Mutua los informes de actuación de la Policía Local y de la ambulancia municipal de la asistencia realizada en su puesto de trabajo a una empleada municipal que posteriormente falleció.
- Cesión de un histórico de bajas laborales por enfermedad de una persona fallecida a sus familiares.
- Cesión de los datos contenidos en un "Libro de Registro de Empadronamiento de Ciudadanos Españoles" y en un "Libro de Empadronamiento de Extranjeros", solicitada por la Comandancia del Puesto de la Guardia Civil de un municipio.
- Cesión de datos obrantes en informes sanitarios de dos menores a los cuales está atendiendo una mancomunidad, debido a las continuas ausencias de los menores a su centro escolar.
- Posibilidad de que una Biblioteca Universitaria implante un servicio de avisos por mensajes SMS para comunicar a los alumnos retrasos en los plazos de devolución de los libros prestados.
- Posibilidad de que por parte del Ayuntamiento se utilicen los datos del Padrón Municipal para "felicitar los cumpleaños" a los vecinos del municipio.
- Cesión de datos sobre absentismo del personal a los representantes sindicales.
- Naturaleza del dato de "objetor de conciencia".
- Utilización de un control de acceso basado en el reconocimiento de la huella digital en un Centro Deportivo Municipal en relación con una niña de tres años que acude al mismo para realizar una actividad de "expresión corporal".
- Actuación de la Comisión de Asistencia Jurídica Gratuita de la Comunidad de Madrid respecto de las peticiones de acceso, realizadas tanto por las partes contrarias de los procedimientos judiciales como por los propios profesionales designados en los mismos, a los expedientes de justicia gratuita derivados de los procedimientos judiciales referentes al reconocimiento del derecho a la asistencia jurídica gratuita.
- Fichero para el control horario usando la huella del personal de un Instituto de Educación Secundaria de la Comunidad de Madrid.
- Acceso a la identidad de la madre biológica de una persona (no se aporta su identidad ni referencia a su minoría o mayoría de edad en la consulta) nacida en un centro hospitalario que fue entregada en adopción y cuya información no figura en su certificado de nacimiento.
- Procedimiento y contenido de los justificantes médicos emitidos por los centros asistenciales de la red sanitaria única de la Comunidad de Madrid.
- Diversas cuestiones relativas a si, de acuerdo con lo previsto en la normativa sobre protección de datos, puede procederse al tratamiento y cesión de los datos personales de las personas víctimas de maltrato o de situaciones de violencia intrafamiliar.
- Posibilidad de cancelar del expediente de un alumno de primer ciclo de Educación Primaria cualquier referencia a las clases de apoyo especial recibidas, a los apoyos relativos a "Psicopedagogía Terapéutica y Logopedia" prestados a dicho alumno y a los informes emitidos en relación con el menor.

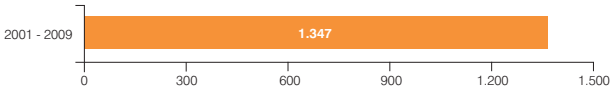
4. ASESORAMIENTO

- Necesidad de crear un nuevo fichero con datos de carácter personal como consecuencia de la "edición electrónica" del *Boletín Oficial de la Comunidad de Madrid*, que comenzará a publicarse el 2 de enero de 2010.
- Análisis del acceso a la información obrante en las cuentas de correo electrónico de los empleados públicos que prestan sus servicios en un Ayuntamiento.

ADMINISTRACIÓN PÚBLICA	NORMAS	CESIONES	ADECUACIÓN LOPD	TOTAL
Vicepresidencia Primera	2	1	1	4
Presidencia, Justicia e Interior	15	2	3	20
Economía y Hacienda	17	0	0	17
Transportes e infraestructuras	0	0	0	0
Educación	28	5	4	37
Medio Ambiente y Vivienda	36	1	1	38
Sanidad	14	17	8	39
Cultura, Deportes y Turismo	1	0	0	1
Familia y Asuntos Sociales	21	1	2	24
Empleo y Mujer	65	1	1	67
Inmigración y Cooperación	9	0	0	9
Organismos Autónomos	0	0	1	1
Otras Instituciones	0	2	4	6
Ayuntamientos	2	20	11	33
Colegios Profesionales	0	2	5	7
Universidades	0	4	1	5
Total	**210**	**56**	**42**	**308**

En total, en el periodo comprendido desde el año 2001 al ejercicio de 2009, la APDCM ha elaborado más de 1300 informes jurídicos sobre disposiciones normativas y consultas planteadas por los responsables de ficheros.

Informes Jurídicos Sobre Disposiciones y Consultas



5. Consultoría

5. Consultoría

5. CONSULTORÍA

En el apartado de Consultoría, la Subdirección General de Consultoría y Registro de Ficheros asume la tarea de asesorar a los responsables de tratamientos de datos personales respecto de la forma más apropiada de implantar las medidas necesarias para dar cumplimiento a lo establecido en la normativa de protección de datos y adecuar sus tratamientos a dicha regulación salvaguardando los derechos de los ciudadanos.

Para el cumplimiento de estos objetivos resulta esencial la figura del "Coordinador de Protección de Datos", persona designada en cada uno de los responsables de ficheros supervisados por la Agencia para que la interlocución sea más eficaz y pueda tanto trasladar a la APDCM sus problemas y dudas como informar a toda la organización de los criterios de la Agencia y las soluciones propuestas. Esta persona ejerce unas funciones similares a las que realiza en el ámbito de las Instituciones Europeas el *"Data Protection Officer"*.

En la planificación anual de la APDCM se plasman, por cada uno de los responsables de fichero, las actuaciones a desarrollar en el año en curso en los diferentes ámbitos de asesoría, entre las que destacan las siguientes:

- creación, modificación y supresión de ficheros;
- regularización de los ficheros existentes;
- formación de los empleados públicos;
- cumplimiento del artículo 5 de la LOPD (derecho de información);
- cumplimiento del artículo 12 de la LOPD (encargado del tratamiento);
- adopción de las medidas de seguridad y documento de seguridad;
- difusión de las instrucciones y recomendaciones aprobadas por la APDCM.

De igual modo, dentro de la actividad correspondiente al año 2009, son dignas de destacarse las diferentes jornadas de formación que se han llevado a cabo y entre las que caben señalarse las dedicadas a la formación de los agentes de las Policías Locales de la Comunidad de Madrid y a la seguridad en el tratamiento de datos personales, contando ambas con una gran asistencia. Asimismo, en esta última jornada se hizo entrega a los asistentes de la publicación de la Agencia de Protección de Datos de la Comunidad de Madrid "Seguridad y Protección de Datos Personales", en la que se ofrece a los responsables de ficheros la información y las directrices necesarias para implantar una política de seguridad que traslade a la práctica los preceptos legales del Reglamento de desarrollo de la LOPD.

Finalmente, tuvo una gran relevancia y trascendencia social la iniciativa puesta en marcha por la APDCM para concienciar a los alumnos de Enseñanza Secundaria de la Comunidad de Madrid de los riesgos que existen para su privacidad en Internet y, especialmente, en las redes sociales. Por su importancia, esta iniciativa se describe pormenorizadamente en el apartado 6 de esta Memoria.

5.1. PLANES SECTORIALES

5.1.1. Videovigilancia

La instalación de sistemas de control basados en la captación de imágenes a través de cámaras de videovigilancia ha experimentado un aumento exponencial en los últimos años. Como consecuencia de ello, los tratamientos de datos personales de imágenes captadas a través de estos dispositivos se han hecho cada vez más comunes y, debido a su especial naturaleza, que no encaja en el concepto tradicional de fichero, se ha hecho necesaria la publicación por parte de la APDCM de una instrucción que clarificara la situación y precisara las obligaciones de las organizaciones que recurran a estos sistemas de vigilancia.

Con este motivo, en el año 2007 la APDCM elaboró y aprobó la Instrucción 1/2007, de 16 de mayo, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones Públicas de la Comunidad de Madrid, con la finalidad de disciplinar y acomodar estos sistemas a las exigencias derivadas del derecho a la protección de datos de carácter personal, haciendo más racional y ordenada la captación, grabación, conservación, elaboración, modificación, bloqueo, cancelación y cesión de las imágenes de las personas físicas realizados por los Órganos y Administraciones Públicas de la Comunidad de Madrid.

Antes de instalar un sistema de videovigilancia, el responsable debe valorar la posibilidad de utilizar un sistema menos intrusivo que la videovigilancia y, en caso de que decida instalarlo, ha de justificar en un informe para la APDCM la necesidad y oportunidad de la instalación de las cámaras de videovigilancia. Posteriormente, tendrá que elaborar y aprobar una disposición de carácter general de creación del fichero; colocar carteles informativos para notificar que se trata de una zona videovigilada en cumplimiento del artículo 5 de la LOPD; establecer un procedimiento para dar respuesta a los derechos de acceso, oposición y cancelación que ejerzan los interesados; y proceder a la cancelación de las grabaciones una vez que hayan transcurrido como máximo 30 días desde la captación de las mismas.

Nº	MANDAMIENTOS DE LA VIDEOVIGILANCIA
1	Valore si puede utilizar un sistema menos intrusivo.
2	Elabore un informe en el que se justifique la necesidad y oportunidad de instalar la videovigilancia.
3	Apruebe la disposición de carácter general de creación del fichero.
4	Coloque un cartel informativo.
5	No utilice las cámaras en aseos o cuartos de baño.
6	Transcurridos como máximo 30 días cancele las imágenes.

Por todo ello, desde la Subdirección General de Consultoría y Registro de Ficheros, se inició en el año 2008 una intensa labor de difusión de los preceptos de la Instrucción con los resultados referidos en la memoria relativa a dicho ejercicio. No obstante, dada la gran cantidad de instalaciones de videovigilancia,

en los responsables de ficheros públicos bajo la supervisión de la APDCM se decidió continuar con el impulso a la regularización de estos sistemas a lo largo de 2009 y, de forma especial, a la notificación de los ficheros correspondientes al Registro de Ficheros de Datos Personales de la Comunidad de Madrid y al cumplimiento del deber de información a través de los preceptivos carteles.

En el Registro de Ficheros de Datos Personales de la APDCM hay inscritos, a fecha de 31 de diciembre de 2009, un total de 88 ficheros de videovigilancia, cuya distribución se presenta en el siguiente cuadro:

FICHEROS DE VIDEOVIGILANCIA INSCRITOS EN EL REGISTRO DE FICHEROS DE LA APDCM	
Ayuntamientos	26
Economía y Hacienda	7
Vicepresidencia, Cultura y Deportes y Portavocía de Gobierno	3
Educación	7
Empleo y Mujer	4
Presidencia, Justicia e Interior	6
Sanidad	26
Transportes e Infraestructuras	3
Familia y Asuntos Sociales	1
Medio Ambiente, Vivienda y Ordenación del Territorio	3
Universidades	3
Total	**88**

Aunque, como se ha comentado, ya en 2008 se realizó un gran avance en la implantación de la Instrucción 1/2007, se incluyen ahora algunos ejemplos significativos de los resultados conseguidos durante el año 2009, segundo año de vigencia del plan.

Entre ellos, se pueden mencionar la declaración y revisión de los sistemas de videovigilancia que, en aras de garantizar la seguridad de las personas y las cosas, se instalaron en las sedes de la Consejería de Presidencia, Justicia e Interior, la Consejería de Transportes e Infraestructuras, la Consejería de Empleo y Mujer y la de Medio Ambiente, Vivienda y Ordenación del Territorio.

En el ámbito de los Servicios Sociales, es de reseñar la declaración de los ficheros de videovigilancia en el Centro Reina Sofía, muchos de cuyos residentes son enfermos de Alzheimer y con cuya instalación se pretende protegerles tanto de amenazas exteriores como de los propios incidentes derivados de su enfermedad.

Dentro del ámbito sanitario, durante el año 2009 se ha completado la tramitación de las disposiciones de carácter general de creación de quince nuevos ficheros de videovigilancia, lo que ha supuesto un incremento del 136% respecto de los ficheros inscritos con esta finalidad en el año anterior. Los nuevos ficheros creados corresponden a las sedes de los servicios centrales de la Consejería y a diferentes centros hospitalarios, así como al Servicio de Urgencia Médicas de Madrid (SUMMA 112) y al Centro de Transfusión de la Comunidad de Madrid.

La instalación de cámaras de videovigilancia en los centros públicos de enseñanza y organismos de la Consejería de Educación ha sido informada favorablemente en aquellos casos en los que se ha constatado que se cumplían los principios de idoneidad (adecuación para el fin perseguido), necesidad (inexistencia de otros métodos para conseguir los mismos fines) y proporcionalidad (preponderancia de intereses generales de importancia que justifiquen la restricción de derechos privados).

Para estas verificaciones se han tenido en cuenta, principalmente, aspectos tales como situación del centro público de enseñanza (descampados, zonas poco concurridas y aisladas, etc.); la reiterada conflictividad en el centro; la existencia de incidentes ocasionados,

como actos vandálicos, destrozos de inmuebles y robos de material didáctico; la entrada al centro educativo de personas ajenas y no autorizadas en horario lectivo; la instalación de cámaras en lugares donde no afecten a los derechos e intimidad de los docentes y alumnos ni al derecho al desarrollo de la libre personalidad de los alumnos, así como el que el número de cámaras sea proporcional al área del recinto del centro de enseñanza. Además, se han declarado e inscrito los sistemas de videovigilancia instalados en la sede central de la Consejería de Educación.

En relación con la Administración Local, la mayor parte de los tratamientos de videovigilancia declarados corresponden a actuaciones de la Policía Local con la finalidad de vigilar los inmuebles públicos que tienen bajo su custodia o para mejorar la seguridad ciudadana en espacios conflictivos. Igualmente, en todos los casos, se ha requerido la justificación de la necesidad de la instalación aplicando estrictamente los principios de idoneidad, necesidad y proporcionalidad.

Especialmente interesante es la declaración del fichero de las grabaciones a través de videocámaras de los cursos, jornadas y eventos, previo consentimiento expreso de los conferenciantes, que se lleva a cabo en el Centro Integral de Formación de Seguridad y Emergencias del Ayuntamiento de Madrid (CIFSE) y que constituye una gran herramienta de formación del personal de emergencias (bomberos, sanitarios, policías, protección civil, etc.).

En el ámbito de Justicia e Interior, son dignas de mención la finalización de la tramitación de la declaración de los ficheros de videovigilancia con fines de seguridad y control de accesos de todas las Sedes Judiciales, Fiscalías y otros edificios al Servicio de la Administración de Justicia de la Comunidad de Madrid, la de las instaladas en los Parques de Bomberos de la Comunidad de Madrid y en los centros de la Agencia de la Comunidad de Madrid para la reeducación y reinserción del menor infractor.

Para finalizar este apartado, hay que reseñar que la Universidad Complutense y la Universidad Autónoma completaron en este ejercicio la tramitación de la declaración de sus respectivos ficheros de videovigilancia con fines de seguridad y control de acceso de sus edificios e instalaciones, que regularizaron mediante sendas disposiciones generales publicadas en el *BOCM*.

5.1.2. SEGURIDAD

5.1.2.1. Regularización de los niveles de seguridad

Con la entrada en vigor del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado mediante el Real Decreto 1720/2007, se concretaron y explicitaron las medidas de seguridad que deberían cumplir los ficheros manuales que contuvieran datos de carácter personal, viniendo a subsanar en este ámbito la carencia del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, ya que en este último solamente se regulaban las medidas de seguridad para ficheros automatizados.

Al establecerse en la nueva regulación los mismos niveles de seguridad —básico, medio y alto— para los ficheros manuales que para los ficheros automatizados, se imponía también la obligación de incluir en la inscripción de los mismos en el Registro de Ficheros de Datos Personales el nivel correspondiente a cada uno de ellos, tal y como se venía haciendo con los ficheros automatizados.

Dado el gran volumen de ficheros manuales que constaban en el Registro de Ficheros de Datos Personales de la Comunidad de Madrid, se hizo necesario diseñar un plan en el que participaron todos los consultores de la APDCM para poner en marcha los procesos de aprobación de las disposiciones de carácter general necesarias para poder asignar el debido nivel de seguridad a estos ficheros, así como para proceder a su posterior inscripción en el Registro de Ficheros de Datos Personales.

Como resultado de este plan, se ha procedido a regularizar completamente a lo largo de 2009 un total de 3872 ficheros, tanto en la Administración de la Comunidad de Madrid como en los Ayuntamientos y otras instituciones de la Comunidad de Madrid. A continuación se puede observar en el cuadro adjunto la distribución de la regularización de ficheros por responsables de ficheros.

RESPONSABLE	FICHEROS
Consejería de Presidencia, Justicia e Interior	54
Consejería de Economía y Hacienda	68
Consejería de Transportes e Infraestructuras	3
Consejería de Educación	2.077
Consejería de Medio Ambiente, Vivienda y Ordenación del Territorio	81
Consejería de Sanidad	1.519
Consejería de Familia y Asuntos Sociales	6
Consejería de Empleo y Mujer	2
Otras Instituciones de la Comunidad de Madrid	3
Total Administraciones de la Comunidad de Madrid	**3.813**
Ayuntamiento de Campo Real	4
Ayuntamiento de El Molar	2
Ayuntamiento de Gargantilla del Lozoya y Pinilla de Buitrago	2
Ayuntamiento de Navarredonda y San Mamés	2
Mancomunidad Valle Medio del Lozoya	1
Ayuntamiento de Pelayos de la Presa	4
Ayuntamiento de Manzanares el Real	1
Ayuntamiento de Montejo de la Sierra	4
Ayuntamiento de La Hiruela	3
Ayuntamiento de Rivas-Vaciamadrid	4
Ayuntamiento de Sevilla La Nueva	3
Ayuntamiento de Villa del Prado	3
Ayuntamiento de Alcalá de Henares	2
Ayuntamiento de Mejorada del Campo	4
Ayuntamiento de Parla	13
Total Ayuntamientos	**52**
Universidad Politécnica de Madrid	4
Universidad Autónoma de Madrid	2
Colegio Profesional de Higienistas Dentales de la Comunidad de Madrid	1
Total otras personas jurídico-públicas	**7**
Total ficheros regularizados	**3.872**

5.1.2.2. Auditorías de seguridad

La legislación en materia de seguridad de los datos de carácter personal establece que los responsables de ficheros están obligados a realizar auditorías bienales de seguridad para verificar que los ficheros con un nivel de seguridad medio o alto y los sistemas de tratamiento de la información y locales donde están ubicados cumplen las necesarias medidas de seguridad.

La Agencia de Protección de Datos de la Comunidad de Madrid, al objeto de verificar esta obligación, remite cada dos años un requerimiento dirigido a todos los responsables de ficheros obligados a la implantación de medidas de seguridad de niveles medio y alto, recordándoles la necesidad de la realización de dichas auditorías y solicitándoles la remisión a la Agencia de los informes con los resultados de las auditorías realizadas.

El último requerimiento de este tipo se produjo en noviembre de 2008 y el análisis de los resultados de auditorías que han sido remitidos a la APDCM a lo largo de 2009 demuestra que han mejorado significativamente en casi todos los aspectos auditados con relación a las auditorías revisadas en el periodo precedente.

El análisis de los resultados de la anterior oleada de auditorías resultó muy complicado, dado que no se introdujo en el requerimiento ninguna norma que obligara a realizar las auditorías con un formato o una metodología unificada, por lo que resultaba difícil el tratamiento uniforme de la información recibida.

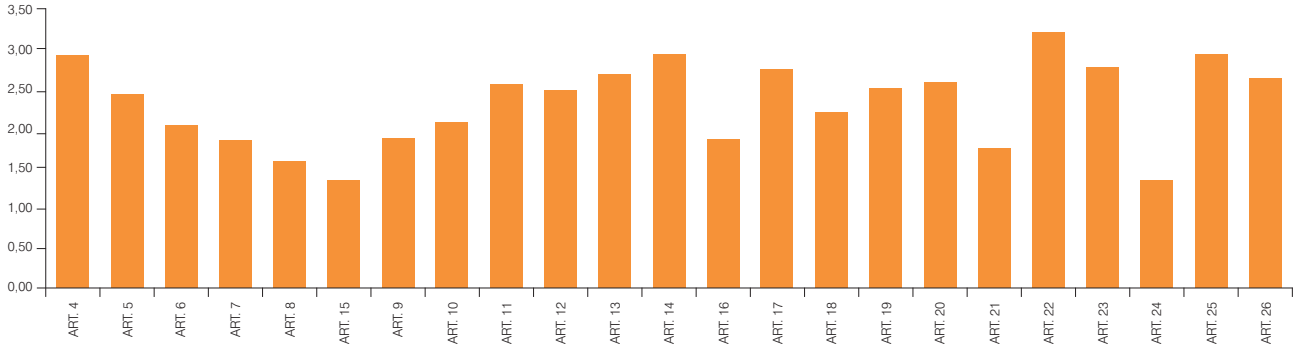
En cambio, en el último requerimiento, aun respetando escrupulosamente la autonomía de los auditores para aplicar aquella metodología reconocida profesionalmente que consideren más apropiada siempre y cuando verificaran todos los aspectos especificados en el Reglamento de desarrollo de la LOPD, se solicitó que al informe de auditoría se adjuntara un resumen de resultados unificado para permitir un mejor tratamiento de la información y una comparación de los datos más objetiva, lo que facilitó el análisis de la información. En la tabla siguiente se incluyen los distintos niveles de valoración utilizados en este resumen.

0	Nulo. Incumplimiento total
1	Cumplimiento muy deficiente. Muchas deficiencias graves
2	Cumplimiento deficiente. Varias deficiencias, algunas graves
3	Cumplimiento normal. Sin comentarios o algunas deficiencias no graves
4	Cumplimiento bueno. Comentario bueno sin ninguna alusión a deficiencias
5	Cumplimiento excelente. Comentario muy bueno

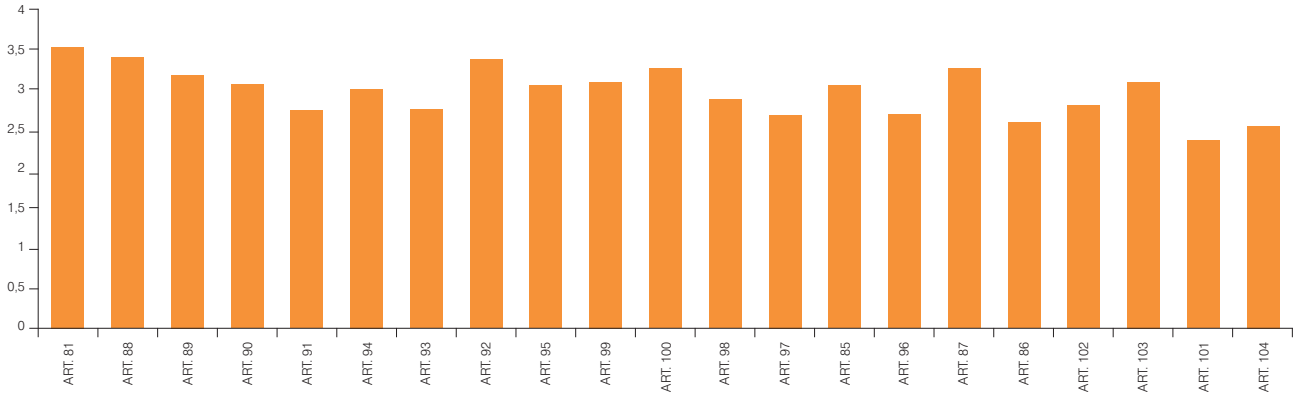
Los resultados de las auditorías fueron analizados con objeto de verificar el grado de cumplimiento de las medidas de seguridad por parte de los responsables y encargados de tratamiento y para analizar las dificultades en este cumplimiento con el fin de detectar los puntos débiles más habituales y trabajar en su subsanación.

A continuación se insertan los gráficos con los resultados de las dos últimas oleadas de auditorías analizadas en los que se aprecia la mejora antes referida.

Resultados de la anterior auditoría



Resultados de la auditoría del año 2009



Como se puede comprobar, aun teniendo en cuenta las diferencias de los reglamentos vigentes, en general, en las auditorías recibidas en 2009 se detecta un grado de cumplimiento notablemente superior al de ocasiones anteriores, aunque sigue habiendo importantes deficiencias en aspectos clave, como los relacionados con el control de acceso e identificación, gestión de soportes y documentos y cifrado de los datos.

5.1.3. Publicación de datos personales en Internet y boletines oficiales electrónicos

La publicación en formato electrónico de los boletines y diarios oficiales en Internet ha supuesto un gran avance en la disponibilidad de la información para un gran número de personas que no la tenían accesible cuando únicamente se publicaban en formato papel. No obstante, esta facilidad en el acceso a la información ha traído como consecuencia, a través de la indexación de los contenidos de los boletines y diarios oficiales que llevan a cabo los distintos motores de búsqueda, la disponibilidad pública y, de

forma prácticamente universal, una miríada de datos relativos a las personas que, en muchos casos, detallan aspectos muy reservados de su vida personal (notificaciones de procedimientos sancionadores, minusvalías, subvenciones, etc.).

Consciente de esta situación, y tras haber recibido numerosas reclamaciones de los ciudadanos, la APDCM aprobó la Recomendación 2/2008 sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios webs institucionales y en otros medios electrónicos y telemáticos, en la que, de una forma sistemática y coherente, se abordaba la aplicación general de los principios de protección de datos a la publicación de datos personales en Internet y su particularización a los distintos tipos de situaciones que llevan aparejada la publicación de datos personales en webs institucionales y, especialmente, en boletines y diarios oficiales.

Uno de los aspectos esenciales tratados en la recomendación es la obligación de los responsables de ficheros de notificar a las instituciones encargadas de la gestión de los boletines y diarios oficiales las solicitudes de cancelación de datos personales estimadas para que se procediera al bloqueo de dichos datos en el boletín o diario oficial correspondiente.

Para impulsar la implantación de la Recomendación y, en particular, de este aspecto sumamente relevante, la Agencia de Protección de Datos de la Comunidad de Madrid mantuvo numerosas reuniones y contactos con el Organismo Autónomo *Boletín Oficial de la Comunidad de Madrid* y con la Agencia de Informática y Comunicaciones de la Comunidad de Madrid para buscar las soluciones técnicas que permitieran que se bloquearan los datos de aquellas personas a las que se les había reconocido el derecho de cancelación y, de esa forma, evitar que siguieran siendo indexadas por los buscadores.

Como fruto de este trabajo se ha producido el bloqueo de los datos de numerosas personas que así lo habían solicitado y que, de esta manera, han visto satisfecho un anhelo que, en muchos casos, les causaba una profunda inquietud y preocupación.

Finalmente, hay que reseñar que la Comunidad de Madrid se ha mostrado sensible a esta problemática y en el Decreto 2/2010, de 28 de enero, del Consejo de Gobierno, por el que se regula la edición electrónica del *Boletín Oficial de la Comunidad de Madrid*, ha introducido una serie de garantías para el correcto tratamiento de los datos personales publicados en el *BOCM*.

Así, en su artículo 9, sujeta a lo establecido en la legislación de protección de datos los servicios prestados mediante la base de datos gratuita que configura el *BOCM* al disponer que "el Organismo Autónomo Boletín Oficial de la Comunidad de Madrid ofrecerá en su sede electrónica una base de datos gratuita que permita la búsqueda, recuperación e impresión de las disposiciones y actos publicados en la edición digital del BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID, con sujeción a lo establecido en la legislación de protección de datos de carácter personal".

Igualmente, y de forma más específica, en su Disposición Adicional Segunda sobre protección de datos de carácter personal, determina que "en el ámbito de sus respectivas competencias, corresponde a los responsables del tratamiento de datos de carácter personal que promuevan la inserción de anuncios en la edición electrónica del BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID determinar la finalidad, contenido y uso de los datos de carácter personal publicados, así como la posibilidad de bloqueo de los mismos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubiera sido efectuada dicha publicación", con lo que no sólo establece de manera obligatoria y vinculante la

posibilidad del ejercicio del derecho de cancelación mediante el bloqueo de los datos, sino que obliga a los responsables que ordenan la publicación de datos personales a establecer el periodo de tiempo durante el cual los datos deben permanecer a disposición de los usuarios del *BOCM* y el momento a partir del cual los mismos deben bloquearse.

La Agencia de Protección de Datos de la Comunidad de Madrid seguirá trabajando a lo largo del próximo año con el Organismo Autónomo *BOCM* e ICM para impulsar el cumplimiento de estos preceptos y del contenido de la Recomendación 2/2008 mediante la implantación en la nueva versión digital del *BOCM* de las medidas técnicas y organizativas que resulten necesarias.

5.1.4. e-Administración en la Comunidad de Madrid

El año 2009 ha sido el del impulso definitivo a la e-Administración en la Comunidad de Madrid y en el que se ha realizado un esfuerzo extraordinario, coordinado y dirigido por la Dirección General de Calidad de los Servicios y Atención al Ciudadano, para dar cumplimiento a lo dispuesto en la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

Dentro de este gran proyecto se ha llevado a cabo una revisión y reingeniería de cientos de procedimientos, algunos de ellos ya ofrecidos a través de medios electrónicos y, en otros casos, ofrecidos por primera vez a través de los canales telemáticos, que han afectado a todos los órganos y organismos de la Comunidad de Madrid.

La Agencia de Protección de Datos de la Comunidad de Madrid ha prestado todo su apoyo a este proyecto y ha colaborado estrechamente con la Dirección General de Calidad de los Servicios y Atención al Ciudadano para aprovechar esta oportunidad para adecuar mejor a la normativa de protección de datos los servicios ofrecidos electrónicamente por la Comunidad de Madrid.

Así, se ha realizado una completa revisión para garantizar que todos los procedimientos electrónicos que recogen y tratan datos de carácter personal tuvieran asociado un fichero inscrito en el Registro de Ficheros de Datos Personales de la Comunidad de Madrid y que dicha inscripción reflejara fielmente la realidad del tratamiento realizado y estuviera ya adaptada a los requisitos del Reglamento de desarrollo de la LOPD.

De esta forma, se ha podido dar el siguiente paso de normalización de las cláusulas informativas de los formularios electrónicos para que se refirieran al fichero correcto y cumplieran con todos los requisitos establecidos en el artículo 5 de la LOPD, de tal manera que los ciudadanos que se relacionan electrónicamente con la Comunidad de Madrid entregaran sus datos personales con todas las garantías.

Igualmente, todos los formularios electrónicos de recogida de datos personales permiten al ciudadano optar por ejercer su derecho a no entregar datos que obraran ya en poder de la Administración o aportarlos directamente, mediante la inclusión de las correspondientes casillas de solicitud del consentimiento, aportando, además, la información adecuada para que el ciudadano decidiera libre e informadamente.

Finalmente, se ha puesto también en marcha un mecanismo de suscripción personalizada a información de servicio de la Comunidad de Madrid, siempre contando con el consentimiento del ciudadano y con la posibilidad de revocar dicho consentimiento en cualquier momento que lo desee.

6. Día Europeo de Protección de Datos

6. Día Europeo de Protección de Datos

6. DÍA EUROPEO DE PROTECCIÓN DE DATOS

La Agencia de Protección de Datos de la Comunidad elaboró en el año 2009 un *Plan de Comunicación en Protección de Datos Personales para Escolares*, dirigido especialmente a aquellos alumnos que se encontraran cursando Enseñanza Secundaria. La finalidad de este Plan era dar a conocer entre los alumnos el derecho fundamental a la protección de datos personales, exponiendo los riesgos a su privacidad que provienen de las modernas tecnologías de la información y las comunicaciones, tratando de que los menores se conciencien acerca de la necesidad de un uso responsable de éstas.

Este Plan, que contó con el respaldo de la Consejería de Educación, se materializó en tres ejes:

- Eje 1: formar al profesorado en la legislación de protección de datos personales desde una perspectiva práctica vinculada a su actividad docente.
- Eje 2: tratar de transmitir a los alumnos la importancia del respeto a la privacidad personal de manera transversal en las distintas materias —Literatura, Historia, Ciencias Sociales, Matemáticas y Tecnología, etc.—, así como en la asignatura de Educación para la Ciudadanía.
- Eje 3: realizar una sesión informativa sobre el riesgo de las tecnologías de la información en los Institutos de Educación Secundaria de la Comunidad de Madrid.

Esta sesión informativa (Eje 3) tuvo lugar el pasado 28 de enero de 2009, coincidiendo con el Día Europeo de la Protección de Datos Personales. La sesión informativa se realizó en los 404 Institutos de Educación Secundaria de la Comunidad de Madrid, recibiendo la sesión informativa un total de 80.000 alumnos de edades comprendidas entre 15 y 16 años.

La sesión informativa fue impartida por más de 60 expertos en la materia de protección de datos (Jueces, Magistrados, Abogados, Juristas) y personal de la Agencia de Protección de Datos de la Comunidad de Madrid (incluyendo al personal administrativo, que también participó en la impartición de la misma).

Para cubrir el resto de Institutos de Educación Secundaria se contó con la colaboración de los orientadores de los mismos, así como tutores y jefes de estudios.

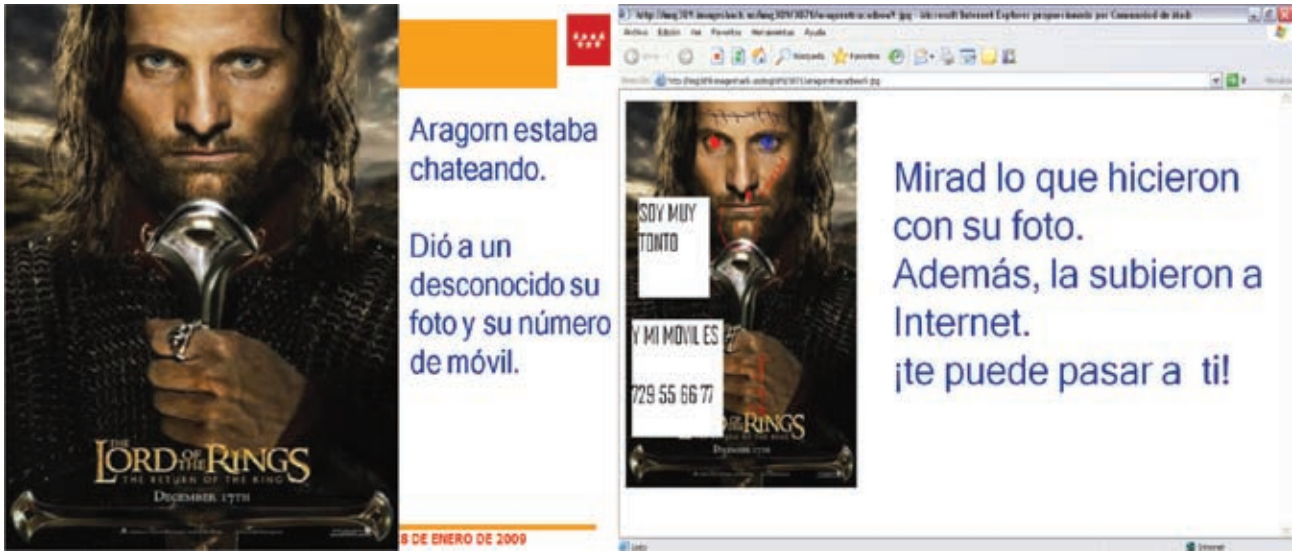
Así mismo, con carácter previo a la impartición de la sesión informativa, personal de la Agencia de Protección de Datos de la Comunidad de Madrid se reunió con directores, jefes de estudios y orientadores de los Institutos de Educación Secundaria para darles la formación necesaria para que pudiesen impartir la mencionada sesión informativa. En este sentido, se celebraron diversas reuniones formativas en las cinco áreas territoriales de educación de la Comunidad de Madrid (norte, sur, centro, este y oeste).

6. DÍA EUROPEO DE PROTECCIÓN DE DATOS

El objetivo de realizar la sesión informativa el 28 de enero de 2009 (Día Europeo de la Protección de Datos Personales) en los 404 Institutos de Educación Secundaria era suscitar un debate acerca de los tratamientos de datos personales que los jóvenes realizan cotidianamente a través del uso de redes sociales, mensajerías instantáneas, chats, telefonía móvil, etc., y de sus consecuencias presentes y futuras, teniendo en cuenta que ninguna información desaparece. Para ello, la sesión estuvo estructurada de la siguiente forma:

- Proyección de seis vídeos ilustrativos a través de los cuales se trataban los problemas de privacidad en las redes sociales, el *cyberbullying*, el pensar antes de publicar *(think before you post)*, lo fácil que es publicar en Internet y lo difícil que es borrar opiniones o fotos de las páginas webs ("efecto Hotel California, es muy fácil entrar, muy difícil salir"), la masiva publicación de fotografías o que nunca sabes con quién estás chateando.
- Exposición de una presentación en PowerPoint con ejemplos ilustrativos de seguridad, *spam*, el uso de la mensajería *(messenger)* o la manipulación de fotos.
- Entrega de Manuales de Protección de Datos elaborados por la organización no gubernamental Comisión de Libertades Informáticas. Estos Manuales constan de tres versiones diferentes: para alumnos de 9 a 11 años, de 12 a 14 años y de 15 a 17 años. A través de los mismos, y mediante el uso de un lenguaje coloquial fácilmente comprensible a la audiencia a la que va dirigido, se reflejan los diferentes problemas que lleva consigo, en la actualidad, el uso de Internet, como es el caso, por ejemplo, del *ciberbullying*, el *spam* o el *phising*.

Esta iniciativa tuvo una gran repercusión en los diferentes medios de comunicación social, tanto en prensa escrita como en Internet y televisión.



Ejemplo de un par de transparencias de la presentación en PowerPoint.


"Piénsalo primero. Luego lo cuelgas"

Diario El País. 29/01/2009.

Sesión informativa en un I. E. S. 28/01/2009.

La campaña se presentó en la Conferencia Europea de Edimburgo que tuvo lugar en esta misma ciudad en abril de 2009 y en la reunión del Grupo de Reclamaciones Transfronterizas de la Unión Europea *(Case Handling Workshop)* celebrado en octubre de 2009 en Limassol. Asimismo, las actividades y resultados de esta campaña van a formar parte de un "Libro blanco" sobre este tipo de actuaciones realizadas por las Autoridades de Control Europeas de Protección de Datos que está preparando la Agencia de Protección de Datos de la República Checa.

Por último, la APDCM también realizó esta misma sesión informativa a más de 100 padres y madres de alumnos, ya que éstos son los primeros que deben conocer los peligros que sus hijos pueden encontrarse en el uso de las tecnologías.

7. Administración Electrónica

7. Administración Electrónica

7. ADMINISTRACIÓN ELECTRÓNICA

7.1. INTRODUCCIÓN

El artículo 6 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, reconoce a los ciudadanos el derecho "a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992, de 26 de noviembre, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos".

En este sentido, la APDCM ha seguido la línea iniciada en el año 2008, en el que se pusieron en funcionamiento el CUMPLE (Sistema de Ayuda al Responsable de Ficheros de Titularidad Pública para el Cumplimiento de sus Obligaciones en Materia de Protección de Datos) y el DEPD (Ejercicio Telemático de Derechos de Protección de Datos).

Así, en el año 2009 se ha procedido a renovar por completo el portal institucional de la APDCM, desarrollando un programa de formación virtual en colaboración con ICM, y, por último, puesto en marcha una herramienta para mejorar las relaciones institucionales por correo electrónico.

7.2. NUEVO PORTAL INSTITUCIONAL DE LA APDCM

El objetivo primordial del nuevo portal institucional de la APDCM es transmitir a los ciudadanos, de una manera mejor y más eficaz, clara y amigable, la actividad y el trabajo de la APDCM en defensa del derecho fundamental a la protección de datos, así como mejorar la información y la concienciación y facilitar el ejercicio de los derechos a través de Internet.

Asimismo, se ha pretendido actualizar y modernizar la interfaz gráfica para mejorar la navegabilidad y hacerla más intuitiva y usable. Para ello, también se ha procedido a reestructurar determinadas secciones e incluir zonas de descargas de audio y vídeo, incluyendo la posibilidad de visualización en formato *streaming*, que antes no existía.

7. ADMINISTRACIÓN ELECTRÓNICA

Para facilitar el acceso a la información que interesa a cada colectivo, se ha procedido a definir siete canales con una denominación clara e intuitiva que anuncia su contenido. En concreto, existe el canal "La Agencia", a través del que se proporciona la información institucional de la misma, su estructura y funciones de los órganos que la componen, así como la carta de servicios, los indicadores de gestión de la APDCM y los convenios de colaboración firmados por la Agencia.

En el canal denominado "Ciudadanos" se exponen de manera clara los principios de protección de datos, así como los derechos que asisten a los ciudadanos y la forma de ejercerlos. Como complemente esencial a esta exposición, el portal proporciona también la posibilidad de ejercer estos derechos a través de Internet utilizando los mecanismos de firma electrónica y registro telemático de la Comunidad de Madrid, así como remitir denuncias y reclamaciones empleando herramientas similares. En este mismo canal también es posible remitir consultas a la APDCM, consultar el Registro de Ficheros y obtener modelos de impresos para aquellas personas que no dispongan de firma electrónica o prefieran ponerse en contacto con la Administración a través de medios tradicionales.

Vista del canal "Ciudadanos".

Por lo que respecta al canal "Responsables de Ficheros", en el mismo se incluye toda la información necesaria para poder notificar los ficheros de datos personales a la APDCM y los formularios necesarios para ello, modelos para los contratos de prestación de servicios por terceros, de pliegos de prescripciones técnicas para la contratación de auditorías de seguridad externas, de documentos de seguridad para ficheros automatizados y manuales. Igualmente, también se proporciona acceso al programa CUMPLE, desarrollado por la APDCM para facilitar a los responsables de ficheros el cumplimiento de sus obligaciones en diversos ámbitos, incluyendo la declaración de ficheros a través de Internet si se dispone de certificados digitales, la gestión de las auditorías de seguridad, la elaboración de los documentos de seguridad y la atención de los derechos ARCO.

Vista del canal "Responsable de ficheros".

En los canales "Eventos y Proyectos" y "Publicaciones" se da cuenta y se anuncian las actividades de la APDCM en estos campos, dando información actualizada sobre los mismos e incluyendo el acceso a las presentaciones y audios de las jornadas y even-

tos formativos organizados por la Agencia, así como el acceso gratuito a las publicaciones digitales de la Agencia *www.datospersonales.org* y *Data Protection Review*.

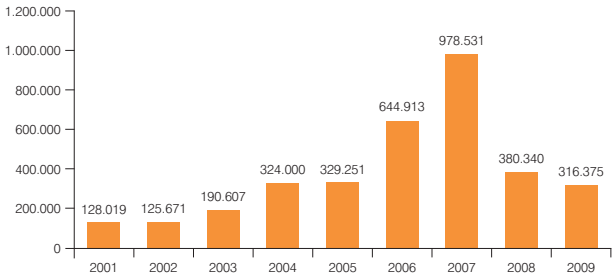
El canal "Legislación y Jurisprudencia" recoge las normas internacionales, nacionales y autonómicas más relevantes en materia de protección de datos, conteniendo las recomendaciones e instrucciones de la APDCM, así como extractos de las sentencias más relevantes de los diferentes tribunales.

Finalmente, en el canal "Consultas y Resoluciones" se incluyen todas las resoluciones dictadas por la APDCM en los procedimientos de infracción y de tutela de los derechos que tramita, así como un resumen de las respuestas que proporciona la Agencia a las consultas más frecuentes o interesantes en cada uno de los sectores de actividad más relevantes que están bajo su supervisión.

En cuanto a los accesos a la página web de la APDCM, durante el año 2008 hubo un total de 316.375 peticiones de acceso (dato facilitado por ICM). Conviene destacar que la disminución de las peticiones de acceso respecto al año 2008 viene motivado por el hecho de que el cambio al nuevo portal institucional supuso que durante tres meses el portal antiguo no se actualizase.

La diferencia de accesos desde el año 2007 a 2008 y 2009, como ya hicimos mención en la Memoria del año 2008 (ver apartado 6.4 de la misma), se justifica por el cambio del sistema de cómputo de las mismas, contando conexiones y no accesos individualizados a las páginas.

Peticiones a la Web de la APDCM
Comparativa de los últimos años



7.3. FORMACIÓN VIRTUAL

Este nuevo curso virtual nace de la voluntad de la Agencia de dar respuesta a las necesidades formativas de los empleados públicos, necesidad que ha aconsejado la preparación, junto con ICM, de una herramienta virtual que permita facilitar aún más la formación en protección de datos personales.

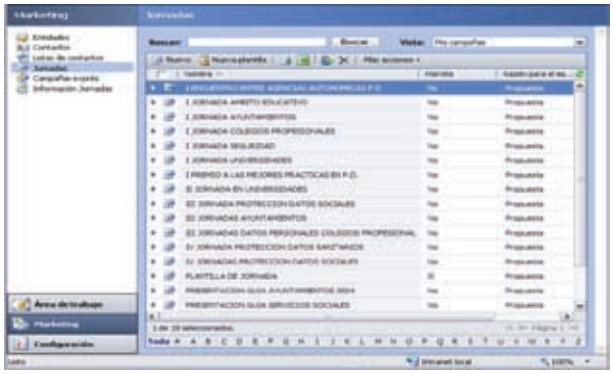
El Programa de Formación Virtual en Protección de Datos Personales consta de 15 horas lectivas y está estructurado en dos grandes bloques: principios y derechos de protección de datos personales y orientaciones prácticas para el cumplimiento de las obligaciones de los responsables y empleados públicos.

El Programa utiliza animaciones para introducir cada uno de sus capítulos, está completamente locutado y propone diversas prácticas y test para ayudar a la comprensión de la materia y comprobar los conocimientos adquiridos. Los alumnos disponen a lo largo del curso del apoyo de tutores que les animarán y ayudarán a resolver las cuestiones y dudas que pudieran surgir. El curso incluye un examen presencial a la finalización del mismo para que los alumnos puedan obtener el correspondiente certificado que acredite que lo han realizado con aprovechamiento.

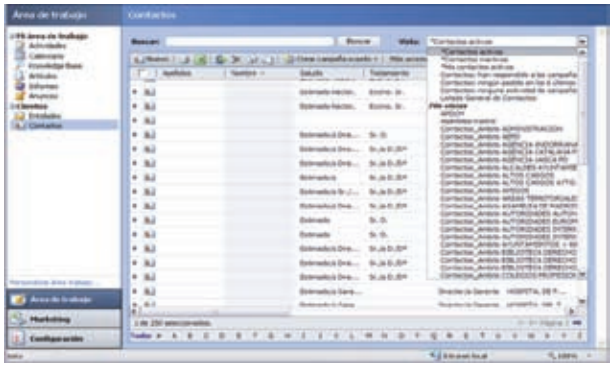
Por último, la APDCM ha recibido 1289 solicitudes de empleados públicos de la Comunidad de Madrid para realizar este curso *on-line*.

7.4. CRM (CUSTOMER RELATIONSHIP MANAGEMENT)

Se trata de un sistema informático cuya principal utilidad es mejorar la gestión de las relaciones institucionales de la APDCM. El *CRM* permite administrar un *data warehouse* (almacén de datos) con toda la información de los contactos institucionales de la Agencia.



Una de las principales utilidades que tiene el *CRM* es que posibilita una mayor eficiencia y eficacia a la hora de gestionar las convocatorias de las diversas jornadas o actos que organiza la APDCM.



8. Formación, difusión y gestión del conocimiento

8. Formación, difusión y gestión del conocimiento

8. FORMACIÓN, DIFUSIÓN Y GESTIÓN DEL CONOCIMIENTO

8.1. JORNADAS Y FORMACIÓN

Desde la creación de la APDCM, uno de sus principales objetivos ha sido facilitar el cumplimiento de la normativa de protección de datos a los responsables de la administración de la Comunidad de Madrid a través del asesoramiento y formación del personal de los centros y servicios públicos.

Para alcanzar este objetivo han sido varias las vías utilizadas por la Agencia: la designación de consultores responsables para el ámbito de educación y, de forma específica y diferenciada, para cada uno de los responsables de ficheros que resuelvan las dudas que puedan plantearse a los gestores públicos; la programación de un exhaustivo programa formativo en diversos niveles; la edición de publicaciones específicas para el ámbito de la educación en todos sus niveles, que se han distribuido de forma gratuita a todos los responsables y en cursos de formación; y, por último, la celebración de jornadas de difusión de determinados contenidos específicos de la normativa de protección de datos, en la que se ha dado participación a diferentes responsables de instituciones dependientes de la Administración de la Comunidad de Madrid, Ayuntamientos, Colegios Profesionales y Universidades.

A las actuaciones referidas en el párrafo anterior habría que añadirse la puesta en funcionamiento del programa de formación virtual, al que ya hemos hecho referencia en el apartado 7.3 de esta Memoria.

En este sentido, las jornadas celebradas durante el año 2009 tuvieron como objetivo dar continuidad a la línea iniciada en el año 2008, es decir, dar a conocer las principales implicaciones del nuevo Reglamento de desarrollo de la LOPD en los diferentes ámbitos sectoriales, presentar las herramientas de Administración CUMPLE, dirigida a facilitar al responsable del fichero el cumplimento de la LOPD, y DEPD, dirigida al ciudadano para que pueda ejercitar los derechos ARCO (acceso, rectificación, cancelación y oposición) telemáticamente. Asimismo, en el ámbito de seguridad se presentó un Manual Sectorial referido a dicho ámbito.

También se ha dado respuesta a uno de los sectores con más demanda, como es el de educación, ya que, si bien en el año 2008 ya se celebró la III Jornada, en el año 2009 se ha celebrado la IV Jornada y también se ha realizado una jornada dedicada exclusivamente a los Departamentos de Orientación de los Institutos de Educación Secundaria.

Como viene siendo tradicional, cada una de las jornadas contó con una mesa en la que los responsables de los ficheros pudiesen describir sus experiencias y la celebración de las mismas tuvo lugar en edificios institucionales relacionados con el público al cual iban dirigidos.

Estas jornadas fueron las siguientes:

PROGRAMA

9:15 Entrega de documentación

9:30 Inauguración

9:45

10:15

10:45

11:15 Descanso

11:45

12:15

12:45

13:30 Coloquio

13:45 Clausura

Objetivos:

Dirigido a:

Lugar de celebración:

Inscripción:

PROGRAMA

9:15 Entrega de documentación

9:30 Inauguración

9:45

10:45

11:15 Descanso

12:15

12:45 Coloquio

13:00

14:00 Clausura

Objetivos

Dirigida a

Lugar de celebración

Auditorio del I.E.S. Beatriz Galindo

C/ Goya, 10

28001 MADRID

Inscripción

PROGRAMA

9:15 Entrega de documentación

9:30 Inauguración

10:00

10:45

11:15 Descanso

11:45

13:15

13:45 Coloquio

14:00 Clausura

Objetivos

Dirigido a

Lugar de celebración

Inscripción

9:30 Entrega de documentación

9:45 Inauguración

Objetivos

- Dar a conocer las implicaciones del nuevo Reglamento de Desarrollo de la LOPD.
- Exponer la situación de los tratamientos de datos, así como los problemas surgidos en la aplicación de las medidas de seguridad.
- Compartir experiencias reales de los tratamientos de datos en el ámbito educativo respecto a la implantación de la normativa. Difundir la experiencia de esta implantación y analizar las dificultades y soluciones adoptadas por parte de los centros de enseñanza.
- Difundir la normativa y los criterios de interpretación sobre protección de datos a los responsables de ficheros.

10:00 La Protección de Datos en el ámbito educativo

10:45 El Reglamento de Desarrollo de la LOPD.

11:45 Descanso

12:15 La experiencia práctica en la orientación educativa

13:15 Consultas frecuentes planteadas en el ámbito de los Orientadores de Programas Educativos

14:00 Clausura

Dirigida a

- Directores de equipos de orientación y atención temprana en sus diferentes organizaciones
- Orientadores
- Tutores
- Personas relacionadas en la información y orientación de menores y jóvenes de diferentes niveles

Lugar de celebración

Salón de actos del I.E.S. Virgen de la Paloma

C/ Ramón Rodríguez, 106

28035 MADRID

ASISTENTES	
IV Jornada Centros Educativos	222
II Jornada de Seguridad	160
II Jornada para Policía Local	145
Jornada para Equipos de Orientación	450

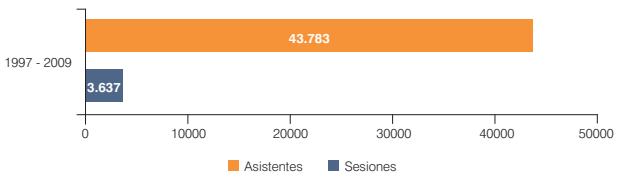
Asimismo, esta labor formativa no sólo se desarrolla a través de las jornadas citadas anteriormente, sino también mediante la celebración de sesiones informativas a los empleados públicos. Estas sesiones informativas pueden tener un contenido general y un contenido específico (por ejemplo, sesiones dirigidas a colegiados, personal sanitario).

INDICADOR	2007	2008	2009
Sesiones informativas	316	305	199
Asistentes a sesiones informativas	3853	3880	3145

La disminución en el número de sesiones informativas y asistentes tiene dos motivos: el primero es la puesta en marcha de la formación virtual (ver apartado 7.4 de esta Memoria), en la que, como ya se ha dicho, se han recibido 1289 solicitudes para hacer este curso *on-line*; el segundo, al haber realizado la APDCM una labor formativa muy intensa desde su fundación, la demanda de la misma por parte de los responsables de ficheros se ha estabilizado o, incluso, disminuido en los últimos tiempos.

De esta forma, durante el periodo 1997-2009, la APDCM ha celebrado un total de 3637 sesiones informativas, a las que han acudido 43.783 empleados públicos.

Sesiones Informativas y Asistentes



Por último, destacar que el personal de la APDCM impartió una jornada específica con una duración de tres días, organizada por la Dirección General de Consumo de la Comunidad de Madrid, a personal de la Administración del Estado, Comunidades Autónomas y Corporaciones Locales que prestan servicio en departamentos de consumo.

8.2. Participación de la APDCM en seminarios

Durante el año 2009 la APDCM ha participado en numerosos seminarios, jornadas y sesiones informativas, tanto a nivel nacional como internacional, a los cuales ha sido invitada para exponer su experiencia como garante del derecho fundamental a la protección de datos de carácter personal. De los mismos, podemos destacar los siguientes:

1. A nivel nacional:

   – Máster en Derecho de las Telecomunicaciones y Tecnologías de la Información. "Los extranjeros y la protección de datos". 21 de enero de 2009. Universidad Carlos III de Madrid.

   – Jornada de Divulgación de Protección de Datos. 5 de febrero de 2009. Organizada por el Ilustre Colegio de Abogados.

   – Seminario "Protección de Datos en las Administraciones Públicas". Ponencia: "La Protección de Datos en la C. M.". 25 de marzo de 2009. Organizado por Socinfo.

   – Conferencia Cooperación Social Guadalajara. Ponencia: "Redes Sociales y Privacidad". 26 de marzo de 2009.

   – Jornadas Tecnológicas de Melilla. Ponencia: "Protección de Datos en las AA. PP.". 15, 16 y 17 de abril de 2009. Organizada por la Consejería de Presidencia y Participación Ciudadana de Melilla.

   – VI Foro sobre Protección de Datos de Salud. 20 y 21 de mayo de 2009. 20 de mayo. Organizado por la S. E. I. S.

   – Nuevos Retos en materia de Protección de Datos. 1.ª Jornada sobre protección de datos: La empresa y la LOPD. Cáceres, 21 de mayo de 2009. Jornada organizada por ADATEX (Asociación de Empresarios de Protección de Datos y Seguridad de la Información de Extremadura).

   – Jornadas Redes Sociales. 16 de junio de 2009. Colegio de Abogados de Madrid.

   – Jornada sobre la Protección de Datos en las AA. PP. 28 y 29 de junio de 2009. 29 de junio de 2009. Organizada por Dintel.

   – Curso Seguridad Telemática 2009. Ponencia: "Agencias de Protección de Datos en las CC. AA.". 2 de julio de 2009. Universidad de Vigo.

   – Presentación pública del *Data Privacy Institute*. 14 de julio de 2009. Clausura. Organizado por ISMS Forum Spain. Salón de Actos. Consejo General de Colegios de Médicos de España.

   – Historia Clínica: confidencialidad y acceso. Ponencia: "La protección de datos y los servicios sanitarios. El nuevo reglamento de protección de datos". 16 de octubre de 2009. Junta de Castilla y León, Consejería de Sanidad.

   – "La gestión documental como garantía del cumplimiento de la LOPD". 27 de octubre de 2010. Mesa redonda organizada por Computerworld.

   – Máster Derechos y Libertades Fundamentales. Curso: Nuevas dimensiones de los derechos. Conferencia: "Protección de Datos Personales, problemas actuales". 19 de noviembre de 2009. Organizado por la Universidad de Castilla-La Mancha. Facultad de Ciencias Jurídicas y Sociales. Toledo.

– Protección de datos y tecnologías de la información en el sector sanitario. XIII Congreso de la Sociedad de Reumatología de la Comunidad de Madrid. 10 de diciembre de 2009.

– Curso de Mediación y Resolución de Cyberconflictos. Menores. Ponencia: "La Protección de Datos en el ámbito educativo". 11 y 12 de diciembre de 2009. Organizado por IAITG y CEU.

2. A nivel internacional:

– Semana Estatal de Transparencia de México. Ponencia: "Protección y Corrección de datos personales como Política de Estado". 27, 28 y 29 de abril de 2009. Organizada por el Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios. Estado de México.

– VI Seminario Internacional sobre Protección de los Datos Personales —Éxitos e Innovaciones— hacia el bicentenario de la República Argentina. Ponencia: "La Protección de Datos Personales en el ámbito regional, nacional e internacional". 14 de mayo de 2009. Organizado por la Dirección Nacional de Protección de Datos Personales del Gobierno de Buenos Aires (Argentina).

– Lanzamiento de la Unidad Reguladora y de Control de Datos Personales. Conferencia sobre Protección de Datos. 15 de mayo de 2009. Salón de Fiestas del Palacio Legislativo. Montevideo (Uruguay).

– Congreso "Privacidade e Protecção de Dados Pessoais". 29 de mayo de 2009. Oporto (Portugal).

– Seminario "Data protection for police and judicial cooperation in criminal matters: EU requirements". 4 y 5 de junio de 2009. Sarajevo (Bosnia-Herzegovina).

– Seminario "Lucha contra el cibercrimen". 28 y 29 de septiembre 2009. Tbilisi (Georgia).

– V Congreso Iberoamericano de Seguridad Informática CIBSI'09. Conferencia: "La protección de datos y el diseño de tratamientos de datos personales. Especificaciones funcionales necesarias". Del 16 al 18 noviembre de 2009. Montevideo (Uruguay).

– Seminario "Data protection for police and judicial cooperation in criminal matters: EU requirements". 10 y 11 de diciembre de 2009. Bucarest (Rumania).

8.3. PREMIOS

8.3.1. Premio Europeo a las Mejores Prácticas Públicas en Protección de Datos. V edición

Este premio europeo, cuya primera edición fue convocada en el año 2004, fue creado por la APDCM con el objetivo de fomentar la sensibilización sobre el derecho fundamental a la protección de datos entre los responsables de ficheros del ámbito de las Administraciones Públicas europeas, así como de los empleados públicos que intervienen en cualquier fase del tratamiento de los datos de carácter personal. Asimismo, el premio reconoce las experiencias o proyectos más sobresalientes en el ámbito europeo, permitiendo, además, que los mismos puedan ser utilizados por otras Administraciones Públicas europeas.

En definitiva, con este premio la APDCM busca la difusión de las mejores prácticas en materia de protección de datos, propuestas o implantadas para el tratamiento de datos por cualquier órgano o institución de la Administración Pública de cualquiera de los países adheridos al Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales.

A continuación, se muestran los galardonados de la V edición.

GALARDONADOS V EDICIÓN

Consejería de Educación de la Comunidad de Madrid. "Creación del registro electrónico de historiales académicos".	Ayuntamiento de Alcobendas. "Alcobend@s protege tus datos".	Asociación de municipios vascos (EUDEL). "Manual de buenas prácticas". Crossroads bank for social security (Bélgica). "Seguridad".

El acto de entrega de los premios de la V edición tuvo lugar el 18 de febrero de 2009 y contó con la participación de numerosos expertos y autoridades europeas y nacionales en protección de datos de carácter personal, así como responsables de los diecisiete proyectos que habían presentado su candidatura.

Los premios fueron entregados por D. Alfonso Cuenca Miranda, Viceconsejero de Justicia y Administraciones Públicas de la Comunidad de Madrid.

Representantes del Excmo. Ayuntamiento de Alcobendas, ganadores de la V Edición del Premio Europeo a las Mejores Prácticas Públicas en Protección de Datos con el proyecto "Alcobend@s protege tus datos".

8.3.2. Premio al Mejor Artículo Científico en Protección de Datos

Mediante la convocatoria de este premio se pretende alcanzar un mayor grado de concienciación ciudadana en relación con "la cultura de la protección de datos", fundamentalmente a través de la transmisión del conocimiento inherente a la difusión de trabajos científicos, técnicos o jurídicos relacionados con la protección de datos de carácter personal.

De esta manera, la Agencia de Protección de Datos de la Comunidad de Madrid pretende potenciar la realización de trabajos de investigación, elaborados en forma de artículo, que, desde un plano jurídico, científico, económico, técnico o social, aborden los aspectos teóricos y prácticos derivados del tratamiento de la información de carácter personal relativa a personas físicas identificadas o identificables.

En consecuencia, los trabajos presentados a este premio deben ser inéditos, versar sobre la protección de datos personales, ya sea desde una perspectiva estrictamente teórica, ya sea abordando el estudio y análisis de experiencias concretas con incidencia sobre esta materia, realizándose dicho análisis con el rigor científico y académico exigido en este tipo de premios.

Si bien se presentaron dos candidaturas a este premio, mediante Resolución de 23 de octubre de 2009 del Director de la APDCM se declaró desierto el mismo.

8.4. FORMACIÓN DE ALUMNOS UNIVERSITARIOS

Si se sigue la línea marcada por año anteriores, y en virtud de los Convenios de Colaboración que tiene firmada la APDCM con las distintas Universidades Públicas de la Comunidad de Madrid, se ha continuado con la formación de alumnos universitarios.

Estas prácticas versan sobre el conocimiento de la normativa de protección de datos, funcionamiento del Registro de Ficheros de la APDC, funcionamiento y organización de Atención al Ciudadano de la APDCM, análisis jurídico del procedimiento de inspección, tutela de derechos y procedimiento sancionador y análisis de las funciones del responsable del fichero. Asimismo, los alumnos realizan casos prácticos e informes jurídicos.

UNIVERSIDAD CARLOS III	
Formación Académica LICENCIATURA EN ESTUDIOS CONJUNTOS (DERECHO)	
PERIODO	ALUMNOS
Marzo/mayo 2009	4
Julio 2009	4
UNIVERSIDAD AUTÓNOMA	
Formación Académica LICENCIATURA DE DERECHO	
PERIODO	ALUMNOS
Abril/mayo 2009	4

8.5. CENTRO DE INVESTIGACIÓN Y DOCUMENTACIÓN "PABLO LUCAS MURILLO DE LA CUEVA"

Mediante Resolución de 28 de enero de 2008, del Director de la Agencia de Protección de Datos de la Comunidad de Madrid, se procedió a crear y poner en funcionamiento el Centro de Investigación y Documentación "Pablo Lucas Murillo de la Cueva" de la Agencia de Protección de Datos de la Comunidad de Madrid.

Con la creación de este Centro se potencia la realización de trabajos de investigación que, desde un plano jurídico, científico, económico, técnico o social, aborden los aspectos teóricos y prácticos derivados del tratamiento de la información de carácter personal relativa a personas físicas identificadas o identificables y abrir una nueva vía para la difusión del derecho fundamental a la protección de datos de carácter personal, creando un espacio especializado que sirva de centro de referencia para que preste servicio no sólo a la Administración Autonómica, sino a otras Administraciones, tanto nacionales como internacionales, y a estudiosos o particulares interesados que necesiten información sobre tan importante derecho como es la protección de datos personales.

Durante el año 2009 se ha ampliado el fondo documental de este Centro con un total de 204 publicaciones, alcanzando en la actualidad un fondo de más de 2000 publicaciones y 20 revistas especializadas.

En este sentido, el 24 de junio de 2009, D. Miguel Ángel Davara donó al Centro de Investigación y Documentación "Pablo Lucas Murillo de la Cueva" 124 libros pertenecientes a su colección privada.

Asimismo, a través de la página web de la APDCM se ha habilitado un enlace para poder realizar consultas sobre el bibliográfico con el que se cuenta.

9. Publicaciones

9. Publicaciones

9. PUBLICACIONES

9.1. SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES

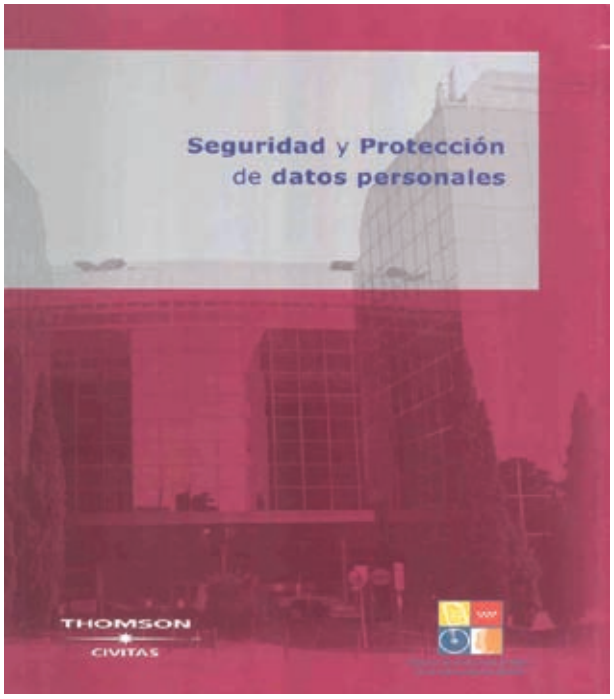
En el año 2009 la APDCM ha elaborado y publicado el manual sectorial "Seguridad y protección de datos personales". El manual está orientado a los responsables de ficheros y responsables de seguridad, que deben conocer las medidas de seguridad aplicables a los administradores informáticos de los ficheros protegidos y, sobre todo, a los usuarios de los datos personales.

Así, se analizan las medidas de seguridad para ficheros automatizados y manuales establecidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/19999, de 13 de diciembre, para facilitar su implantación y cumplimiento, analizando los riesgos y las amenazas que conlleva el estado actual de la tecnología, recomendando unas normas de conducta para el personal que maneja los datos protegidos.

El Reglamento, dado que es una norma legislativa, solamente especifica la obligación de cumplir unas determinadas medidas, sin explicar cuáles son los fundamentos o peligros por los que son imprescindibles esas medidas. Esto es así porque, por su propia naturaleza, las leyes o normas legislativas no suelen profundizar en las causas de las que deriva la necesidad de esas normas, sino que tan sólo proceden a citarlas someramente y a enumerar las obligaciones o medidas que son de obligado cumplimiento.

Es fundamental que los usuarios y administradores de los datos personales estén advertidos de cuáles son los peligros y amenazas y qué pueden hacer cada uno de ellos para defender la seguridad de los datos que tienen bajo su responsabilidad. Este es, pues, uno de los objetivos de esta publicación: presentar de una forma inteligible para el nivel medio de los usuarios las técnicas que actualmente se utilizan para atacar la seguridad de los datos y exponer cuáles son los "mejores hábitos" (o *best practices* en inglés) para defenderse de esos ataques.

Con esta publicación se sigue la línea iniciada en el año 2008 con las publicaciones de los manuales sectoriales *Protección de datos personales para Servicios Sanitarios Públicos, Protección de datos personales para Administraciones Locales, Protección de datos personales para Universidades Públicas, Protección de datos personales para Servicios Sociales Públicos, Protección de datos personales en Corporaciones de Derecho Público* y *Protección de datos personales en Centros Educativos Públicos* y con la publicación *Guía de Protección de datos personales para Empleados Públicos.*



9.2. REVISTAS

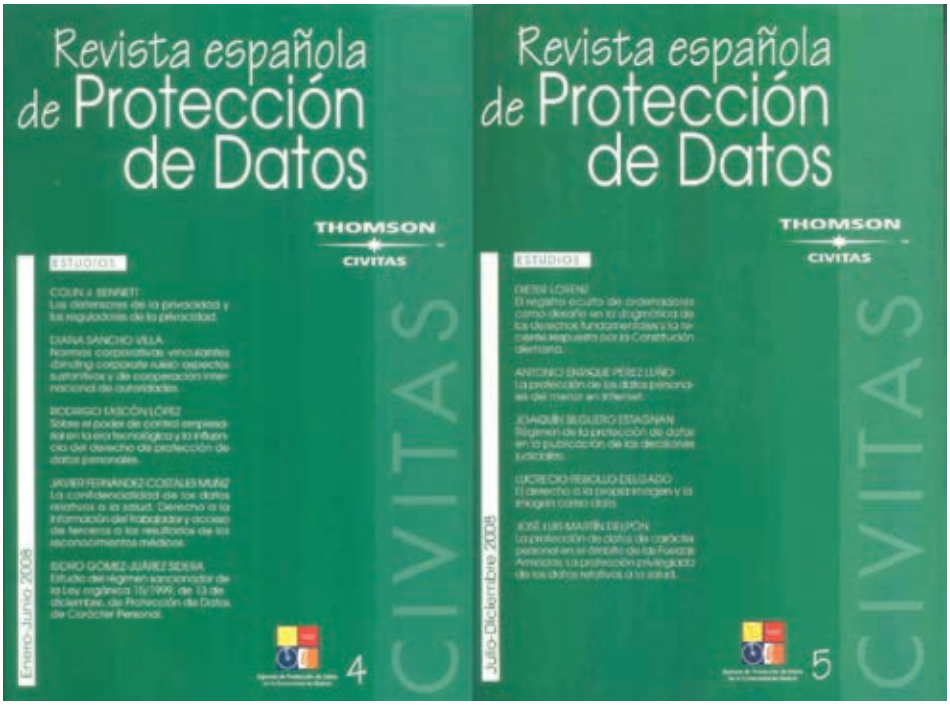
9.2.1. Revista Española de Protección de Datos

En el año 2007 se puso en marcha la *Revista Española de Protección de Datos (REPD)*, que dirige la APDCM y que edita Thomson-Civitas, con la finalidad de dar a conocer aquellos artículos doctrinales, bien desarrollados desde el punto de vista científico, sobre el derecho fundamental a la protección de datos.

La *Revista Española de Protección de Datos* es una revista preferentemente *jurídica* que estudia el ordenamiento de protección de datos personales y que enjuicia la actividad de los poderes públicos y de los particulares. No obstante, la protección de datos personales es un ámbito donde están presentes y entran en conflicto claramente determinados intereses y valores, donde se observan los problemas que plantea proteger ámbitos de libertad informática al tiempo que se permite la actividad de las Administraciones Públicas y de las empresas. Por ello, la revista no se cierra en el análisis *lege lata*, sino que pretende estar atenta a las demandas de la sociedad en este ámbito, aportando propuestas de *lege ferenda* y ofreciendo a los tribunales criterios de interpretación de las normas jurídicas que tengan en cuenta la eficacia de las distintas soluciones. Esta revista tiene vocación de aportar materiales no sólo para el conocimiento de las normas jurídicas, sino también para el diagnóstico de los problemas y para las propuestas de solución en aras de alcanzar una sociedad más justa. Por ello, a través de esta revista se publican aquellas reflexiones de *ciencia política* que pretenden justificar con rigor y sin demagogia qué valores deben primar en los distintos supuestos. Con esto se favorece la reflexión entre quienes defienden opiniones y tienen convicciones distintas acerca de la protección de datos personales, contribuyendo de alguna manera a comprender —a interiorizar— los distintos intereses en juego.

La revista, con una periodicidad semestral, dispone de las secciones de “Estudios”, “Comentarios de Legislación y Jurisprudencia”, “Reseñas bibliográficas”, “Documentos” y “El Foro”. Se ha establecido un Comité de Redacción del que forman parte profesores que desde distintas áreas de investigación –Derecho administrativo, Derecho penal, Derecho del trabajo, Derecho civil, Derecho internacional, Derecho constitucional, Derecho sanitario– desarrollan un trabajo sistemático de evaluación de los contenidos.

En el año 2009, se han publicado los números 4 y 5 de la *Revista Española de Protección de Datos*.



Con el objetivo de comprobar si la *Revista Española de Protección de Datos* puede ser considerada o no una publicación de impacto científico, ha sido sometida a un riguroso estudio por parte de uno de los miembros del Comité Evaluador de la misma. Fruto de este estudio son las modificaciones reflejadas a partir del cuarto número de la revista. Una vez hechas dichas modificaciones, se solicitó su inclusión en bases de datos internacionales y especializadas, para lo cual fue objeto de un proceso de valoración por parte del Centro de Ciencias Humanas y Sociales del Consejo Superior de Investigaciones Científicas, orientado a seleccionar para la base de datos ISOC aquellas publicaciones que superen un determinado umbral de calidad editorial e interés científico-técnico.

La valoración fue positiva y la *Revista Española de Protección de Datos* ha sido considerada de impacto científico, por lo que ha sido admitida e incluida con la categoría C-Normal.

9.2.2. Revista digital *www.datospersonales.org*

Creada en marzo del año 2003, la revista digital *www.datospersonales.org* se ha convertido en referente en materia de publicaciones que abordan de manera exhaustiva y pormenorizada, desde diferentes vertientes, el derecho fundamental a la protección de datos de carácter personal.

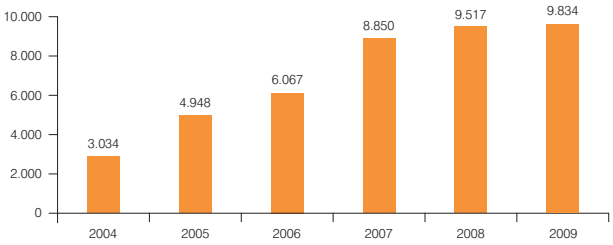
9. PUBLICACIONES

Esta revista digital, de periodicidad bimensual, cuenta en la actualidad con 42 números publicados, habiéndose publicado durante el año 2009 un total de seis números.

Los artículos publicados por los expertos en el citado año 2009 han versado, entre otros, sobre cuestiones tan diversas como pueden ser los peligros invisibles de la privacidad en Internet, extranjeros y protección de datos, SITEL, investigación en salud médica y derecho a la intimidad, presente y futuro de las medidas de seguridad y el juez de control de garantía frente al tratamiento de datos personales.

Asimismo, se ha seguido reforzando el resto de contenidos de la revista (noticias nacionales e internacionales, normativa nacional e internacional, jurisprudencia y publicaciones), destacando el canal referente a jurisprudencia internacional, en donde se han analizado por expertos en la materia el Auto del Tribunal Constitucional 155/2009/2009, de 18 de mayo de 2009, de inadmisión de recurso de amparo núm. 1682/2007, el cual se fundamenta en la supuesta vulneración del derecho fundamental a utilizar los medios de prueba pertinentes para su defensa y del derecho fundamental a comunicar o recibir información veraz por cualquier medio de difusión, y la Sentencia del Tribunal Constitucional 159/2009, de 29 de junio, recurso de amparo 9914-2006, sobre cesión de datos de salud en el marco de un proceso selectivo.

Nº de suscriptores **Evolución anual de suscriptores**



9.2.3. Revista digital *www.dataprotectionreview.eu*

La Agencia de Protección de Datos de la Comunidad de Madrid puso en marcha en octubre de 2006 la publicación digital en inglés *Data Protection Review (www.dataprotectionreview.eu)*, habiéndose publicado durante el año 2009 tres nuevos números.

El objetivo de *www.dataprotectionreview.eu* es facilitar la difusión de la cultura de protección de datos a todas aquellas personas interesadas profesionalmente en los aspectos jurídicos y técnicos de la misma y que tienen como primer o segundo idioma la lengua inglesa. De esta forma, la revista está dirigida a una amplia audiencia internacional formada por los miembros y empleados de las autoridades de protección de datos, profesores universitarios, estudiantes, profesionales, funcionarios públicos, abogados, organizaciones no gubernamentales y todas aquellas personas interesadas en tener información actualizada sobre privacidad y protección de datos.

Para ello, *www.dataprotectionreview.eu* se estructura en cinco canales:

1. *Commissioner's Corner* (La Tribuna del Comisionado): Reservada para que los comisionados, presidentes o directores de las autoridades de control de protección de datos puedan expresar su opinión en relación con aquellos temas que les preocupen o sobre los que sus autoridades hayan trabajado especialmente. Así, durante los números publicados en el año 2009, hemos podido leer en este canal los siguientes artículos:
   - The guantanamisation of data. Natasa Pirc Musa. Information Commissioner of the Republic of Slovenia.
   - Would the personal data be protected when court decisions are published and made available? Marijana Marusic. Director (Directorate for Personal Data Protection of Macedonia).
   - The Federal Institute of Access to Public Information as the Guarantor Entity for the Protection of Personal Data. Jacqueline Peschard. Representative President of the Federal Institute for Access to Public Information of Mexico (IFAI).

2. *Experts' opinion* (La opinión de los expertos): Como su nombre indica, contiene artículos de expertos en la materia. Han participado en ella, entre otros:
   - Communications and External Relations Strategy in the Information Commissioner's Office (ICO). Susan Fox. Director of Communications and External Relations Information Commissioner's Office (United Kingdom).
   - Organizational Motives for Adopting Privacy Enhancing Technologies (PETs). John Borking. Former data protection commissioner of The Netherlands. Owner/director of Borking Consultancy in Wassenaar (The Netherlands).
   - Recent Developments in Israeli Data Protection Law: En Route to European Standards. Omer Tene. Associate Professor, College of Management School of Law and legal consultant.
   - Open Space Privacy Dialogue at PrivacyOS Conferences. Katalin Storf. PrivacyOS Project Coordinator. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD).
   - Data protection auditing, problematic and challenges. Dina Kampouraki. Leading auditor in the Greek Data Protection Authority.
   - Are Users of Social Networking Sites Subject To Data Protection Law, As Controllers? Douwe Korff. Professor of International Law. London Metropolitan University. London (UK).
   - What Outcomes Should Regulation Achieve for Individuals, Regulators and Society? Charles Raab. Professor Emeritus and Honorary Professorial Fellow, School of Social and Political Science, University of Edinburgh.
   - Social Networking Sites and Freedom of Expression. Douwe Korff. Professor of International Law. London Metropolitan University. London (UK).

3. *In the last four months* (En los últimos cuatro meses): Esta sección pretende proporcionar a los lectores un resumen con los acontecimientos más importantes e interesantes que han sucedido en el mundo en relación con la privacidad y la protección de datos.

4. *Regulation and Case Law* (Regulación y Jurisprudencia): Referencias, reseñas y comentarios sobre nuevas leyes y normativa, así como sobre

jurisprudencia de todos los niveles: regional, nacional, europeo o internacional.

5. *Decisions and Opinions* (Resoluciones y Dictámenes): En ella tienen cabida las resoluciones, dictámenes, directrices, instrucciones o recomendaciones de interés general que produzca cualquier autoridad de protección de datos en el mundo y que sean de interés general para la comunidad internacional de protección de datos.

9.3. MONOGRAFÍAS DE PROTECCIÓN DE DATOS

Siguiendo la línea iniciada en 2003 de participación e impulso de iniciativas que contribuyan doctrinalmente a desarrollar y analizar la problemática que se deriva del derecho fundamental a la protección de datos personales, iniciativas con indudable interés didáctico y doctrinal, la Agencia coeditó en 2009 una nueva monografía con la Editorial Aranzadi-Civitas dentro de la colección “Protección de Datos”.

9.4. DÍPTICOS SECTORIALES DE INFORMACIÓN SOBRE PROTECCIÓN DE DATOS

El objetivo de estos dípticos, cuyo destinatario son los ciudadanos que utilizan los servicios públicos que prestan las diferentes Administraciones Públicas, es que éstos tengan un mayor conocimiento de su derecho fundamental a la protección de datos personales.

Por esta cuestión se ha utilizado en los citados dípticos un lenguaje sencillo y directo, de manera que los ciudadanos puedan conocer los derechos que le asisten en esta materia.

Además, puesto que los dípticos se han elaborado para los usuarios de los centros sanitarios y de los centros de servicios sociales, el contenido de los mismos se ha adaptado a las peculiaridades de cada sector.

En este sentido, se han editado y distribuido por los diferentes centros, tanto de servicios sanitarios como de servicios sociales, 35.000 ejemplares del díptico de protección de datos personales para servicios sanitarios públicos y 15.000 ejemplares del díptico de protección de datos personales para servicios sociales.

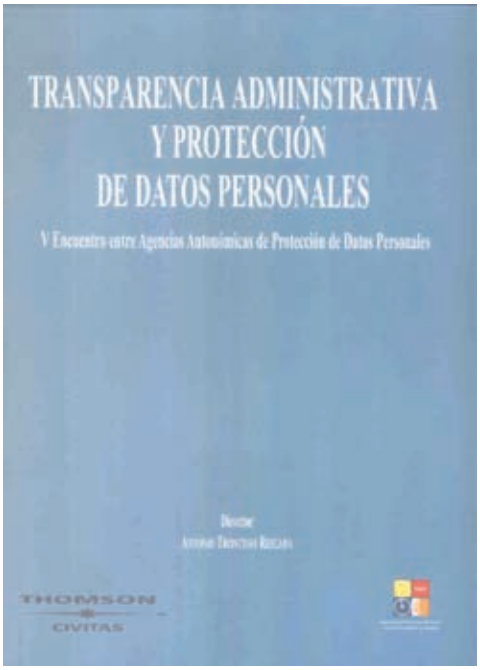
9.5. TRANSPARENCIA ADMINISTRATIVA Y PROTECCIÓN DE DATOS PERSONALES

Este libro recoge las ponencias del V Encuentro entre Agencias Autonómicas de Protección de Datos celebrado en Madrid el 28 de octubre de 2008. Esa jornada fue una oportunidad para analizar cuáles debían ser los criterios que permitan alcanzar un adecuado equilibrio entre la transparencia administrativa y el derecho fundamental a la protección de datos personales.

Este libro aborda la cuestión desde un planteamiento doctrinal con la participación de distintos académicos, se analiza la citada cuestión desde una perspectiva comparada con la contribución de diferentes Autoridades de Control que asumen al mismo tiempo la competencia de protección de datos personales y la garantía del acceso a la información pública, cuenta también con la participación y opinión de los portavoces de los grupos parlamentarios en la Comisión de Administración Pública del Congreso de los Diputados así como de la sociedad civil.

Además, puesto que el V Encuentro entre Agencias Autonómicas de Protección de Datos fue una buena oportunidad para analizar el Reglamento de desarrollo de la LOPD, en el libro se encuentran las ponencias dadas por los empleados públicos de las cuatro Agencias de Protección de Datos que existen en España en el marco del citado encuentro.

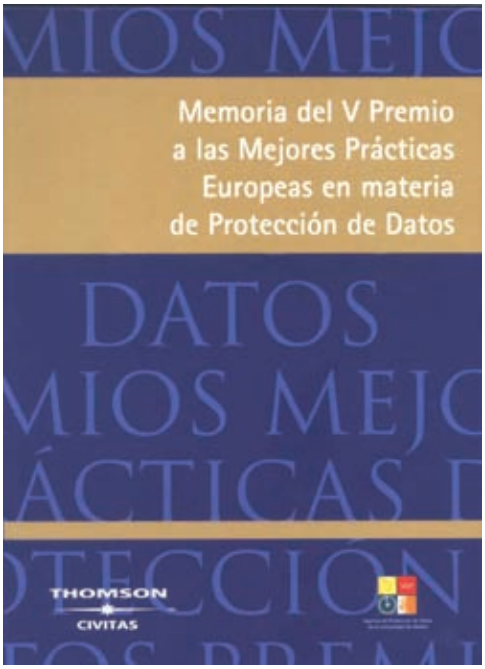
El libro *Transparencia administrativa y protección de datos personales* fue presentado en la sede de la APDCM el 17 de septiembre de 2009 en un acto presidido por el Viceconsejero de Justicia y Administraciones Públicas de la Comunidad de Madrid, en el que intervinieron, además del Director de la APDCM, los Directores de la Agencia Española de Protección de Datos, la Agencia Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos.



9.6. Memoria de la V Edición del Premio a las Mejores Prácticas Europeas en materia de Protección de Datos

Recoge no sólo las candidaturas presentadas a la V Edición del Premio, que fueron un total de diecisiete, sino también las candidaturas presentadas a las cuatro ediciones anteriores de este premio.

De esta forma, y puesto que el premio tiene como finalidad no sólo reconocer el esfuerzo de las diferentes Administraciones Públicas que hayan implantado la protección de datos personales en sus procesos, sino la transferencia del conocimiento a través de la Memoria de la V Edición, los responsables de ficheros pueden utilizar las diferentes candidaturas presentadas para adecuar sus respectivos procedimientos a la protección de datos personales. En otras palabras, utilizar la gestión del conocimiento.



10. Atención al ciudadano

10. Atención al ciudadano

10. ATENCIÓN AL CIUDADANO

El Área de Atención al Ciudadano de la Agencia de Protección de Datos de la Comunidad de Madrid está encuadrada dentro de las Oficinas de Información Especializada que conforman el Sistema de Información horizontal de la Comunidad. El objetivo prioritario de este servicio es proporcionar a las personas información y orientación acerca de los derechos reconocidos en la normativa vigente en materia de protección de datos de carácter personal, contribuyendo en la difusión de este derecho fundamental.

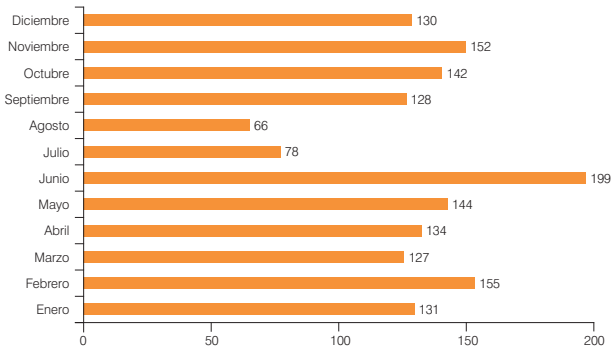
Esta Área depende jerárquicamente de la Secretaría General en virtud de lo establecido en el artículo 20 del Decreto 40/2004, de 18 de marzo, por el que se aprueba el Estatuto de la Agencia.

El Área de Atención al Ciudadano, como ya se ha manifestado en anteriores Memorias, supone la primera fuente de aproximación de que dispone el ciudadano para obtener información sobre los principios y derechos relativos a las personas recogidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), en la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad de Madrid, y sobre el resto del ordenamiento jurídico de aplicación en esta materia.

Al objeto de cumplir con las funciones descritas anteriormente, el Área de Atención al Ciudadano de la Agencia de Protección de Datos de la Comunidad de Madrid pone a disposición del ciudadano distintos cauces:

- A través del correo electrónico *apdcm@madrid.org*.
- A través de la revista digital *www.datospersonales.org*.
- A través del teléfono 91 580 28 74/75.
- A través del fax 91 580 28 76.
- Atención presencial y mediante correo ordinario en la sede de la Agencia de Protección de Datos de la Comunidad de Madrid, ubicada en la calle Cardenal Marcelo Spínola, n.º 14, 28016, Madrid.

El número total de consultas atendidas durante el año 2009 fue de 1586.



10. ATENCIÓN AL CIUDADANO

Gráfico 1. Análisis por Tema

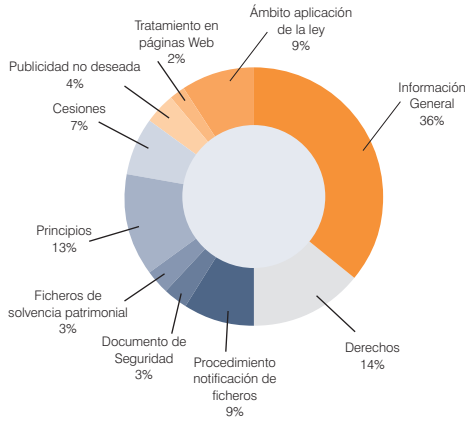
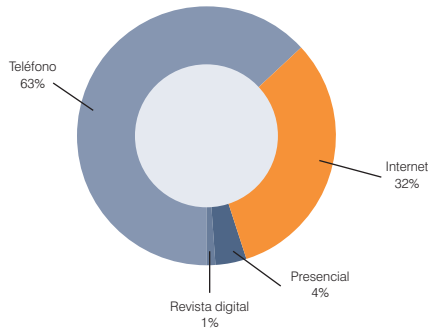


Gráfico 2. Análisis por Medio



Entre todas las consultas, podemos destacar por su relevancia las siguientes:

- La información que deben contener en cumplimiento de la LOPD los impresos utilizados por la Administración de la Comunidad de Madrid en los que se recogen datos de carácter personal.
- Si es posible publicar los datos personales en el *Boletín Oficial de la Comunidad de Madrid* y que, a su vez, sean recogidos por un buscador, quedando a disposición de cualquiera.
- La solicitud de una farmacia a un centro de salud de los datos de un paciente para ponerse en contacto con él y poder comunicar que ha habido un error en la medicación suministrada.
- Aplicación de la LOPD a los representantes de personas jurídicas.
- Cuando un hospital deniega el acceso a la historia clínica, cuáles son los trámites a seguir.
- Solicitud de un paciente a su médico para anonimizar sus datos personales.
- Publicación de una institución en su web de los acuerdos de sus órganos colegiados de gobierno que incluyan nombre y apellidos del interesado.
- Aplicación de la LOPD a los expedientes administrativos en formato papel.
- Posibilidad de visionar las imágenes de una cinta de video mediante la cual, presuntamente, se podría inculpar al autor de una sustracción.
- Legalidad de una encuesta que pregunta sobre datos de salud, incluidos los de familiares, para participar en una competición universitaria.

11. Colaboración entre la APDCM y otras Autoridades e Instituciones de control

11. Colaboración entre la APDCM y otras Autoridades e Instituciones de control

11. COLABORACIÓN ENTRE LA APDCM Y OTRAS AUTORIDADES E INSTITUCIONES DE CONTROL

11.1. GRUPO DE TRABAJO ENTRE AGENCIAS

En el marco del principio de lealtad institucional que preside las relaciones entre las distintas Agencias de Protección de Datos existentes en el territorio nacional (Agencia Española de Protección de Datos, Agencia Catalana de Protección de Datos, Agencia Vasca de Protección de Datos y Agencia de Protección de Datos de la Comunidad de Madrid), se han creado diversos Grupos de Trabajo con el objetivo de aunar posturas interpretativas y debatir sobre aquellas cuestiones que estén de actualidad. En este sentido, los Grupos de Trabajo existentes son los siguientes:

- Directores.
- Registro, coordinado por la Agencia Española de Protección de Datos.
- Inspección, coordinado por la Agencia de Protección de Datos de la Comunidad de Madrid.
- Análisis Jurídico y Normativo, coordinado por la Agencia Catalana de Protección de Datos.
- Organización, Modernización, Comunicación y Formación, coordinado por la Agencia Vasca de Protección de Datos.

11.1.1. Grupo de Trabajo de Directores

Los Directores de las Agencias de Protección de Datos se reúnen para marcar las líneas estratégicas de colaboración entre las autoridades de control, hacer el seguimiento de las mismas y culminar el proceso de toma de decisiones sobre los asuntos que se han debatido en los distintos grupos y que requieran la aprobación de la dirección para su implantación y puesta en marcha.

Durante el año 2009 los Directores de las Agencias se reunieron en la sede de la APDCM el 17 de septiembre de 2009, en la cual se informó por cada responsable de las reuniones mantenidas en los otros grupos durante el citado año.

Asimismo, se trataron, entre otros, aspectos relacionados con la 31.ª Conferencia Internacional, que fue organizada por la AEPD, la adopción de los Estándares Internacionales de Privacidad, la problemática actual de publicación de datos personales en boletines y diarios oficiales y las novedades que ha implicado el Reglamento de desarrollo de la LOPD en los Registros de Ficheros de las respectivas Agencias.

11.1.2. Grupo de Trabajo de Registro de Ficheros

A lo largo del año 2009 se han celebrado dos reuniones del Grupo de Trabajo de Registro de Ficheros, ambas por videoconferencia.

Entre las cuestiones tratadas por este Grupo podemos destacar las siguientes:

- Revisión de las actuaciones de intercambio de información entre Registros.
- El nuevo sistema RENO: intercambio de ficheros entre Registros a través de *Web Services*.
- Documento de Análisis Funcional "Intercambio de Información Registral entre RGPD y Agencias de CC. AA.".

11.1.3. Grupo de Trabajo de Inspección

Durante 2009 este Grupo de Trabajo se ha reunido en cuatro ocasiones. Dos de las reuniones se han celebrado de manera presencial, una en la Agencia de Protección de Datos de la Comunidad de Madrid y otra en la sede de la Agencia Catalana de Protección de Datos. Las otras dos reuniones se realizaron de manera conjunta con el Grupo de Trabajo de Análisis Jurídico y Normativo, teniendo lugar una de las reuniones mediante videoconferencia y la otra de manera presencial. Los dos grupos se reunieron de forma conjunta debido a que se trataron cuestiones que afectaban a ambos.

La APDCM, como coordinadora de este Grupo de Trabajo, se encarga tanto de la confección del orden del día como de la redacción de las actas de las reuniones.

En el seno del Grupo se han tratado, entre otras, las siguientes cuestiones:

- En relación a los procedimientos de tutela de derechos, sistema de distribución de responsabilidades respecto a la indexación automática que efectúan los buscadores de Internet de la información que se publica en los boletines o diarios oficiales.
- Identificación por DNI de funcionarios de correos en aviso de recibo.
- Naturaleza de los ficheros de las Juntas de Compensación.
- Cuando el afectado interpone simultáneamente una denuncia y una reclamación de tutela de derechos en relación a los mismos hechos, posibilidad de tramitar a la vez un procedimiento de tutela de derechos y una fase de información previa/procedimiento sancionador.
- Responsabilidad médico/empresa sobre documentación clínica.
- Naturaleza de los ficheros de Colegios Profesionales sobre "seguimiento de actividad colegial de depósitos" y "seguimiento de actividad colegial en materia de subastas".
- Inscripción de ficheros de investigación clínica de hospitales.
- Naturaleza de los ficheros con datos utilizados por un polideportivo municipal cuando se procede a gestionar el servicio mediante un contratista privado.
- En relación con las informaciones que aparecen en las publicaciones informativas de las Administraciones Públicas, posible conflicto entre la libertad de información y/o principio de transparencia y el deber de secreto.
- Análisis de la acumulación de procedimientos (artículo 73 de la Ley 30/1992) y la protección de los datos personales.
- Posibilidad de que las Agencias puedan tutelar el ejercicio de los derechos de rectificación y cancelación respecto de los datos obrantes en las historias clínicas de fallecidos, cuando esta tutela es solicitada por los familiares.

- Notificaciones de las Agencias a través de empresa de mensajería.
- Remisión de notificaciones telemáticas a los interesados en los supuestos en que los destinatarios de dichas notificaciones no reúnan los requisitos establecidos en los artículos 13 a 16 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

11.1.4. Grupo de Trabajo de Análisis Jurídico y Normativo

En el año 2009 este grupo se ha reunido en cuatro ocasiones: dos mediante videoconferencia y otras dos, como ya nos hemos referido anteriormente, de manera conjunta con el Grupo de Trabajo de Inspección.

Entre las cuestiones tratadas por este Grupo, podemos destacar las siguientes:

- Aplicación del artículo 2.3 del Reglamento de desarrollo de la LOPD a los ficheros de las Cámaras de Comercio con datos de sus electores. Posibilidad de supresión de los ficheros "Censo electoral de empresas", "Censo público de empresas" y "recurso cameral permanente".
- Alcance del artículo 20.1, último párrafo del Reglamento de desarrollo de la LOPD.
- Condición de fichero o no fichero de los boletines oficiales.
- Concepto de persona identificable (AVPD).
- Revelación del número de DNI con ocasión de la firma electrónica de documentos por parte de funcionarios y autoridades de las Administraciones Públicas.
- Alcance del artículo 35.3 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, en relación con los artículos 6.2.b) y 9 de la misma ley.
- La actuación de las entidades de crédito como entidades colaboradoras de las Administraciones para la recaudación de tributos. El procedimiento recaudatorio y la responsabilidad de las Administraciones.
- Instalación de cámaras de control visual en instalaciones municipales por una empresa de seguridad no autorizada.
- Determinación de los titulares del derecho de acceso a las historias clínicas de personas muertas.

11.2. CONVENIOS Y ACTIVIDAD DE COLABORACIÓN

11.2.1. Convenios firmados

Siguiendo con la tradicional línea de colaboración institucional de la APDCM, cuyo objetivo consiste en establecer las adecuadas fórmulas de cooperación con otras instituciones para promover el desarrollo de programas conjuntos para lograr una mayor difusión del derecho fundamental a la protección de datos de carácter personal, la APDCM ha firmado los siguientes instrumentos de cooperación:

- Convenio de Colaboración entre el Instituto de Acceso a la Información Pública del Distrito Federal y la Agencia de Protección de Datos de la Comunidad de Madrid.
- Convenio de Colaboración entre el Instituto Estatal de Acceso a la Información Pública del Estado de Oaxaca y la Agencia de Protección de Datos de la Comunidad de Madrid.

- Convenio de Colaboración entre el Instituto de Transparencia y Acceso a la Información Pública del Estado de México y municipios y la Agencia de Protección de Datos de la Comunidad de Madrid.
- Convenio marco de Colaboración entre la Fundación Dintel y la Agencia de Protección de Datos de la Comunidad de Madrid.

Asimismo, y de conformidad con una de las cláusulas establecidas en el último de los convenios anteriormente citados, la APDCM se encarga de la sección de "protección de datos" de la revista *DINTEL Alta Dirección –a+)) auditoría y seguridad*.

Por último, se han iniciado los trabajos para firmar los correspondientes Convenios de Colaboración con la Asociación Profesional Española de la Privacidad, la Comisión de Protección de Datos en Andalucía de la Asociación Andaluza de Comercio Electrónico y el Data Privacy Institute.

11.2.2. Reuniones con otras autoridades de control

La APDCM ofreció el 6 de noviembre de 2009, aprovechando la celebración de la 31.ª Conferencia Internacional de Protección de Datos, una recepción en su sede a los miembros de la Red Iberoamericana de Protección de Datos.

En este sentido, la APDCM presentó a los miembros de esta Red sus principales actividades, facilitando la adquisición por parte de éstos de las publicaciones que realiza esta Agencia.

Asimismo, se procedió a la firma de los Convenios de Colaboración con las Instituciones Iberoamericanas referidas en el apartado anterior de esta Memoria.

11.3. CONFERENCIAS DEL DIRECTOR EN MÉJICO, ARGENTINA Y URUGUAY

El Director de la APDCM impartió distintas Conferencias en México, Argentina y Uruguay durante una visita de trabajo que tuvo lugar en el mes de mayo de 2009.

En el transcurso de su visita a México tuvo la oportunidad de reunirse con distintas Instituciones de Acceso a la Información, así como asistir a una sesión plenaria para comprobar sus métodos de trabajo sobre las reclamaciones relacionadas con el acceso a documentos públicos y la protección de datos personales.

El Director, invitado por la Autoridad de Protección de Datos de Argentina, participó en el Sexto Seminario Nacional e Internacional "La Protección de Datos Personales: Éxitos e Innovaciones hacia el Bicentenario de la República Argentina" con una conferencia sobre "La protección de datos personales en el ámbito regional, nacional e internacional: nuevas y mejores prácticas".

Finalmente, la última etapa de su viaje le llevó a Uruguay, donde participo en el VI Seminario Internacional sobre Protección de los Datos Personales "Información Pública y Privada. Aspectos Tutelares y Penales", en donde disertó sobre el Régimen Jurídico de las Bases de Datos Públicas, así como en los actos de celebración del establecimiento y puesta en marcha de la Unidad Reguladora y de Control de Datos Personales, la nueva autoridad de protección de datos establecida en la reciente ley de protección de datos de Uruguay.

12. Actividad Internacional

12. Actividad Internacional

12. ACTIVIDAD INTERNACIONAL

12.1. 31.ª CONFERENCIA INTERNACIONAL DE PROTECCIÓN DE DATOS

La APDCM participó en la sesión paralela "Autoridades subnacionales, subestatales o federadas de protección de datos y Administraciones Públicas: experiencias y estrategias proactivas en educación y salud".

La sesión, moderada por el Comisario de Protección de Datos del Estado de Berlín, contó también con la participación de la Agencia Vasca de Protección de Datos, la Agencia Catalana de Protección de Datos, el Comisario de Privacidad de Québec, la Comisaria de Privacidad de Victoria (Australia), la Comisaria de Privacidad de Ontario y el Comisionado Ciudadano del Instituto de Acceso a la Información Pública del Distrito Federal de México.

El Director de la APDCM se refirió en su exposición a las actividades realizadas en los últimos tiempos por esta Agencia, destacando las diversas actuaciones llevadas a cabo para "promulgar" la cultura de protección de datos. Entre ellas, citó las nuevas publicaciones *Protección de Datos Personales para Servicios Sanitarios, Protección de Datos Personales para Servicios Sociales, Protección de Datos Personales para Educación, Protección de Datos Personales para Universidades Públicas, Protección de Datos Personales para Corporaciones de Derecho Público, Protección de Datos Personales para Administraciones Locales, Seguridad y Protección de Datos Personales, Guía de Protección de Datos Personales para empleados públicos*, las revistas digitales *www.datospersonales.org* y *www.dataprotectionreview.eu* y la publicación científica *Revista Española de Protección de Datos*.

Asimismo, durante la celebración de la Conferencia Internacional la APDCM contó con un *stand* en el cual se daba información de estas actividades y se entregaba documentación y publicaciones a los asistentes.

12.2. EUROPRISE

El Sello Europeo de Privacidad certifica que un producto o servicio cumple con la legislación europea de protección de datos y de privacidad, lo cual supone un valor añadido al citado producto o servicio, además de una garantía para los consumidores.

El Sello de Confianza EuroPriSe *(www.european-privacy-seal.eu)* se emite por una autoridad independiente de certificación a productos y servicios TIC después de haber superado con éxito un procedimiento de evaluación y verificación en dos fases: una evaluación por expertos técnicos y jurídicos acreditados es verificado por una autoridad de certificación independiente e imparcial, la Autoridad de Protección de Datos de Schleswig-Holstein (Unabhaengiges Landeszentrum fuer Datenschutz o ULD). El sello, así como los informes públicos, ofrecen orientación transparente a la hora de elegir o evaluar desde el

punto de vista de la protección de datos un producto o servicio TIC.

En el marco del Seminario EuroPriSe, organizado por la APDCM, celebrado el 3 de noviembre de 2009 en Madrid y enfocado a tratar especialmente temas relativos al trabajo de las autoridades de protección de datos, se concedieron dos nuevos Sellos Europeos de Privacidad. Los mismos fueron entregados por el Director General de Asuntos Europeos y Cooperación con el Estado, don Antonio González Terol, y doña Kirsten Bock, Project Manager del sello EuroPriSe.

El sello fue otorgado al Ilustre Colegio de Abogados de Madrid (ICAM) por su "Solución para la gestión del servicio de Justicia Gratuita" y a la compañía española Iberemec S. A. por su sistema de gestión de relaciones con los clientes "Iberemec CRM". Estos dos servicios TIC demostraron satisfactoriamente su cumplimiento de los exigentes requisitos de la legislación europea de protección de datos.

Entrega del Sello EuroPriSe al Ilustre Colegio de Abogados de Madrid (ICAM) por su "Solución para la gestión del servicio de Justicia Gratuita".

Entrega del Sello EuroPriSe a Iberemec S. A. por su sistema de gestión de relaciones con los clientes "Iberemec CRM".

12.3. PRIVACY OPEN SPACE (PRIVACYOS)

PrivacyOS es un proyecto europeo liderado por Unabhängiges Landeszentrum für Datenschutz (Autoridad de Protección de Datos de Scheleswig-Holstein), y en el que participa la APDCM, que pretende establecer una red temática sobre la creación de infraestructuras de protección de la privacidad. La articulación de esta red se llevaría a efecto a través de la celebración de una serie de conferencias que seguirían el modelo *Open Space*. *Open Space* es una metodología desarrollada en 1985 y ampliamente usada por las ONG, empresas y organizaciones internacionales. Su elemento principal es permitir el desarrollo y modificación de los órdenes del día mientras se celebra la reunión. El objetivo final es establecer una colaboración a largo plazo a través de la red temática y poner en marcha conexiones con otros proyectos europeos.

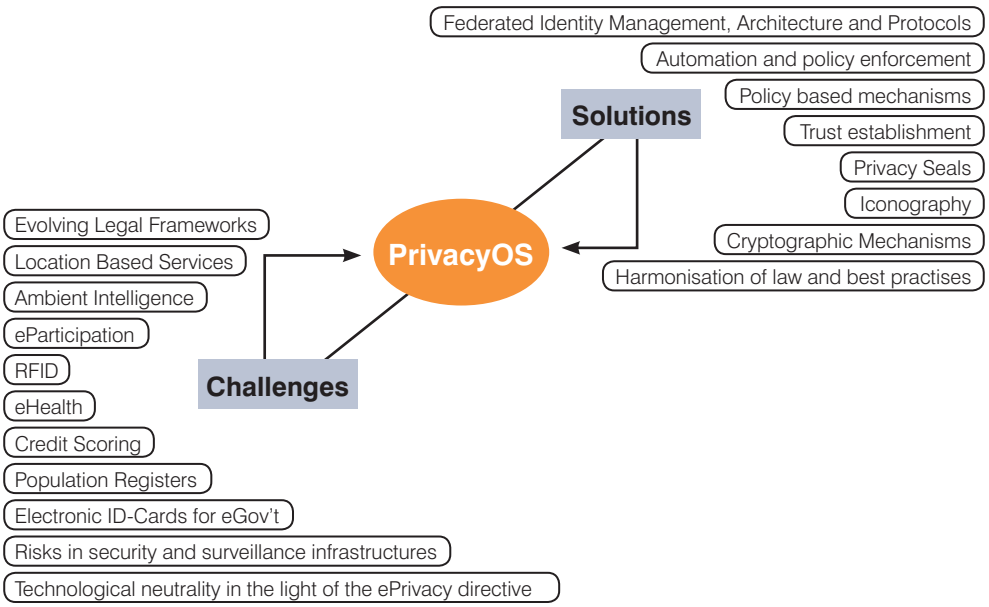
En el año 2009 se han celebrado la Segunda y Tercera Conferencia de PrivacyOS. En la primera, que tuvo lugar en Berlín los días 1, 2 y 3 de abril, la APDCM presentó los resultados del Plan de Comunicación en Protección de Datos para Escolares (ver apartado 6 de esta Memoria).

En esta Segunda Conferencia, a la que asistieron representantes de diez países, se trataron temas de actualidad, se presentaron proyectos piloto y se analizaron los resultados obtenidos en el caso de proyectos ya consagrados. Algunos de los temas tratados fueron: "el valor de la privacidad en la red", "definición y redefinición de PET", "el uso de redes sociales entre menores", "control de acceso selectivo en las redes sociales", "la red de respuesta rápida", "la iconografía al servicio de la privacidad", "el cobro electrónico en carretera: privacidad" o "la encriptación en la Web 2.0".

Respecto a la Tercera Conferencia, que se celebró en Viena los días 26 y 27 de octubre, la APDCM moderó la mesa denominada "Estrategias de la Autoridades de Control de Protección de Datos", que contó con la participación de la Autoridad de Protección de Datos de Eslovenia.

En la misma mesa, uno de los representantes de la APDCM impartió una conferencia sobre las actividades que realiza la misma para crear una cultura de protección de datos, incidiendo no sólo en las publicaciones, sino también en la labor de apoyo al responsable del fichero, destacando el reciente lanzamiento de la aplicación informática CUMPLE.

Durante la conferencia se trataron también temas como el spam y el cibercrimen y se presentaron proyectos como Encore (que trata sobre el procedimiento para otorgar y revocar el consentimiento), TOR (proyecto *software* que le ayuda a defenderse contra el análisis de tráfico, una forma de vigilancia de la red que amenaza la libertad personal) y EuroPriSe.



12.4. PRIMELIFE

La APDCM ha sido elegida e invitada a participar en este Grupo de Referencia por su intensa actividad en muchos proyectos europeos y su experiencia en la promoción, concienciación y supervisión de la protección de datos personales para garantizar que este derecho fundamental se considera debidamente en el proyecto.

PrimeLife, proyecto que continúa la senda iniciada con el Proyecto Prime (ver apartado 11.3 de la Memoria 2008), tratará de dar solución a cómo proteger la privacidad en las aplicaciones emergentes de Internet y cómo conseguir que dicha protección se mantenga a lo largo de nuestra vida.

El Grupo de Referencia está formado por expertos procedentes de diversos campos y realiza una labor consultiva para proporcionar una visión externa, objetiva e independiente a los socios del proyecto para que puedan validar sus avances y resultados con el fin de que la sociedad pueda obtener el máximo beneficio de los productos y servicios que aparezcan como resultado del mismo.

12.5. CONFERENCIAS Y GRUPOS DE TRABAJO DE AUTORIDADES INTERNACIONALES DE CONTROL

12.5.1. Conferencia de Primavera de Autoridades de Protección de Datos

En esta Conferencia, celebrada en Edimburgo en abril de 2009, el Director de la APDCM realizó una exposición sobre los resultados del Plan de Comunicación para Centros Escolares (ver apartado 6 de esta Memoria).

Asimismo, durante la Conferencia se presentaron los puntos principales del informe "Revisión de la Directiva de Protección de Datos" que había encargado la Autoridad Británica de Protección de Datos *(Information Commissioner)* al adjudicatario del concurso convocado al efecto.

Dicho informe suscitó un vivo debate entre todos los asistentes sobre las conclusiones del mismo y, en particular, sobre si es necesario o no abordar o iniciar el proceso de modificación del actual marco jurídico de protección de datos en la Unión Europea.

Del mismo modo, también se abordó el contexto internacional de la regulación en materia de privacidad y, en concreto, D. Artemi Rallo, Director de la Agencia Española de Protección de Datos, expuso el estado de los trabajos que la AEPD está liderando con vistas al establecimiento de un estándar internacional en materia de protección de datos que pueda facilitar los intercambios de información en un mundo globalizado.

Finalmente, la Conferencia aprobó sendos documentos sobre liderazgo en materia de protección de datos en Europa y sobre la necesidad de estableci-

miento de estándares comunes en las transferencias internacionales a terceros países en el ámbito de la cooperación policial y judicial, así como la celebración de la Conferencia del próximo año en Praga (República Checa).

12.5.2. Grupo de Trabajo de Tratamiento de Quejas de la Unión Europea

La APDCM ha participado en las dos reuniones de este grupo que tuvieron lugar en Praga, los días 12 y 13 de marzo de 2009, organizada por la Autoridad de Protección de Datos de la República Checa, y en Chipre, los días 22 y 23 de octubre en Limassol, organizada por la Autoridad de Protección de Datos de Chipre. En la primera reunión, la APDMC presentó en una mesa dedicada a la videovigilancia la Instrucción 1/2007, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los órganos y Administraciones Públicas de la Comunidad de Madrid. En la segunda, los resultados del Plan de Comunicación para Centros Escolares (ver apartado 6 de esta Memoria).

12.5.3. Grupo de Trabajo de Telecomunicaciones

La 45.ª Reunión del Grupo de Berlín se celebró en Sofía los días 12 y 13 de marzo, a la cual asistieron representantes de la APDCM.

Los principales temas incluidos en la Agenda de la 45.ª Reunión fueron los siguientes:

- Tratamiento de datos personales para la persecución de violaciones de derechos de autor en redes p2p.
- Privacidad y e-basura/e-reciclaje.
- Tecnologías de inspección profunda de paquetes y de privacidad.
- Propuesta de una carta de protección de datos digitales y de libertad de información.
- Recabar los recursos necesarios para una estrategia de ciberdefensa en el ámbito de la protección de datos en las telecomunicaciones.
- La "vida privada-consciente de la web".
- CCTV en autobuses y taxis.
- Cuestiones de privacidad en las redes sociales.
- Evaluación del impacto de privacidad: estudios de caso.

Como conclusiones de la reunión se adoptaron dos documentos finales:

- Un informe de recomendaciones sobre tratamiento de datos personales en carreteras de pago (Memorando de Sofía).
- Un informe de recomendaciones sobre Protección de Datos y e-basura.

12.5.4. VII Encuentro Iberoamericano

La APDCM fue invitada por primera vez a participar en el Encuentro Iberoamericano. El mismo tuvo lugar en Madrid, organizado por la Agencia Española de Protección de Datos, y con carácter previo a la celebración de la 31.ª Conferencia Internacional.

En el VII Encuentro se presentaron diferentes ponencias sobre la legislación aplicable de protección de datos personales en Iberoamérica.

13. Secretaría General

13. Secretaría General

13. SECRETARÍA GENERAL

La gestión de los medios personales, económicos y materiales se realiza por la Secretaría General de la APDCM. Junto a estas funciones, podemos destacar también las siguientes:

1. Ejercer la Secretaría del Consejo de Protección de Datos. En el año 2008 se procedió a la renovación de los miembros del Consejo, por haber transcurrido el plazo de nombramiento establecido en el art. 17.3 de la Ley 8/2001 (Decreto 28/2008, de 18 de diciembre, *BOCM* de 23 de enero de 2009), habiéndose realizado la sesión constitutiva el 3 de marzo de 2009. En la actualidad, el Consejo está integrado por los siguientes miembros:

   a) La Asamblea de Madrid: un representante de cada grupo parlamentario.

      – Ilustrísimo señor don Álvaro González López, por el grupo Parlamentario Popular.

      – Ilustrísima señora doña Rosa Alcalá Chacón, por el Grupo Parlamentario Socialista.

      – Ilustrísimo señor don Luís Otero Fernández, por el Grupo Parlamentario de Izquierda Unida.

   b) La Administración de la Comunidad de Madrid: cinco representantes designados por la Presidenta.

      – Ilustrísimo señor don Alfonso Cuenca Miranda, Viceconsejero de Justicia y Administraciones Públicas de la Consejería de Presidencia, Justicia e Interior.

      – Ilustrísimo señor don Borja Sarasola Jáudenes, Secretario General Técnico de Vicepresidencia y Portavocía del Gobierno.

      – Ilustrísima señora doña Zaida María Sampedro Préstamo, Directora General de Sistemas de Información Sanitaria de la Consejería de Sanidad.

      – Ilustrísimo señor don Eugenio López Álvarez, Director General de los Servicios Jurídicos de la Vicepresidencia y Portavocía del Gobierno.

      – Ilustrísimo señor don Amador Sánchez Sánchez, Director General de Calidad de los Servicios y Atención al Ciudadano de la Vicepresidencia y Portavocía del Gobierno.

   c) Las Entidades locales de la Comunidad de Madrid: dos representantes designados por la Federación de Municipios de Madrid.

      – Ilustrísimo señor don Adolfo Rivas Morillo, Alcalde de Orusco de Tajuña.

      – Don Jorge Calderón Hernández, Concejal de San Sebastián de los Reyes.

   d) Un representante de las organizaciones sindicales, elegido por el Consejo Económico y Social de la Comunidad de Madrid.

      – Don Daniel López Montesinos.

e) Un representante de las organizaciones empresariales, elegido por el Consejo Económico y Social de la Comunidad de Madrid.

– D. Luís Méndez López.

f) Un experto en la materia designado por la Asamblea de Madrid.

– Don Germán Alonso-Alegre Fernández de Valderrama.

2. Llevar el inventario de bienes y derechos que integren el patrimonio de la Agencia. A 31 de diciembre el inventario se compone de 844 bienes con un valor inicial de 666.407,32 €.

3. Notificar las resoluciones del Director de la Agencia. Durante el año 2009 se han notificado un total de 272 resoluciones.

4. La difusión de datos y publicaciones, incluyendo, en particular, la memoria de actividades de la Agencia, así como la puesta en funcionamiento del nuevo portal institucional web y las publicaciones electrónicas de la Agencia.

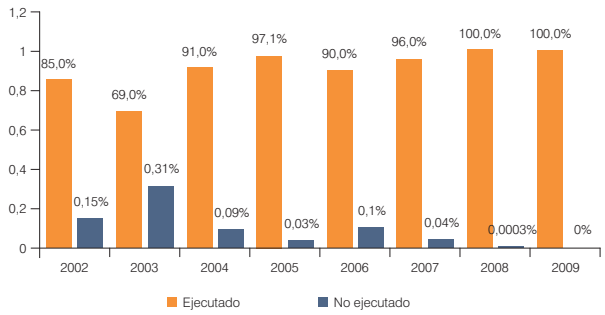
5. La gestión de los fondos documentales de la Agencia y, en particular, la formación y actualización de un fondo de documentación sobre legislación, jurisprudencia y doctrina en materia de protección de datos personales y cualesquiera materias conexas. Hay que destacar que se ha aumentado el fondo documental del Centro de Investigación y Documentación Pablo Lucas Murillo de la Cueva.

6. Organizar conferencias, seminarios, jornadas sobre protección de datos en la Comunidad de Madrid, así como colaborar en las actividades de cooperación internacional o interregional que se le requieran a la Agencia. La Secretaría General se ha encargado de la organización de todas las jornadas y eventos reflejados en esta memoria.

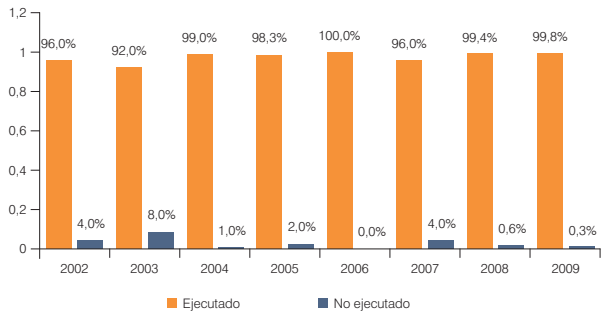
7. Las relaciones institucionales con diversas instituciones para firmar convenios de colaboración, así como el estudio y redacción del contenido de los mismos.

Asimismo, y en lo referente a la gestión económica del presupuesto de la APDCM, hay que destacar el alto nivel de ejecución alcanzado en el ejercicio 2009, que ha sido del 100% del presupuesto de gastos asignado a este organismo.

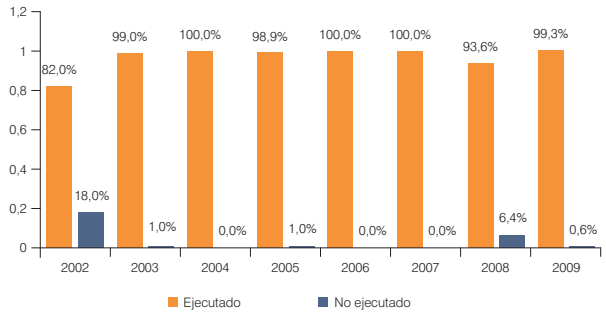
Capítulo I



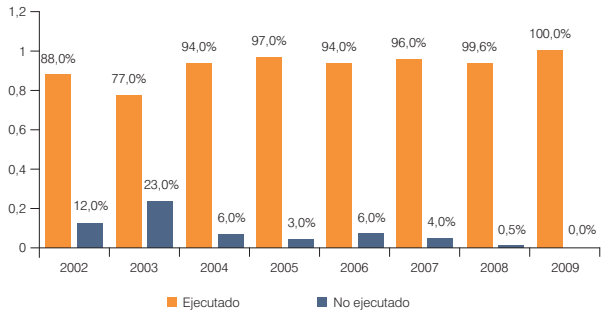
Capítulo II



Capítulo VI



Total programa 125



Agencia de Protección de Datos
de la Comunidad de Madrid

annual report 2009

Agencia de Protección de Datos
de la Comunidad de Madrid

annual report 2009

Published by: AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID

D.L.: M. XXXX-2010
Printed by: B.O.C.M.
ISSN: 1888-8682

Design and layout: ARTEGRAF, S.A.

Contents

Presentation 5

1. Data Register 7

2. Control of Files. Protection of Rights and Inspection 15
   2.1. Administrative Procedures 17
      2.1.1. Introduction 17
      2.1.2. Protection of Rights 17
      2.1.3. Inspection Proceedings 18
   2.2. Inspection Plans 20
      2.2.1. Introduction 20
      2.2.2. 2008-2010 inspection plan on compliance with data protection regulations when collecting the said data via the web pages of the Town Councils of the Madrid Region 20
3. Regulatory Development 21
   3.1. Introduction 23
   3.2. Recommendation 1/2009, of 17 December 2009, on the personal data processing of newborn babies in the health centres forming part of the single public health system of the Madrid Region (*BOCM* of 21 January 2010) 23
   3.3. Recommendation 2/2009, of 21 December 2009, on the processing of personal data when issuing medical certificates 24
4. Assessment 25

5. Consultation 31
   5.1. Sector Plans 34
      5.1.1. Video Surveillance 34
      5.1.2. Security 36
         5.1.2.1. Regularisation of Levels of Security 36
         5.1.2.2. Security Audits 38
      5.1.3. Publication of Personal Data in the Internet and Official Electronic Journals 39
      5.1.4. e-Administration in the Madrid Region 41

6. European Data Protection Day 43

7. e-Administration 49
   7.1. Introduction 51
   7.2. The APDCM's New Institutional Portal 51
   7.3. Virtual Training 53
   7.4. CRM (Customer Relationship Management) 54

8. Training, Dissemination and Knowledge Management 55
   8.1. Conferences and Training 57

CONTENTS

8.2. APDCM Participation in Seminars 60
8.3. Awards 61
8.3.1. European Award for Best Public Practices in Data Protection. 5th Edition 61
8.3.2. Award for the Best Scientific Paper on Data Protection 63
8.4. Training University Students 63
8.5. "Pablo Lucas Murillo de la Cueva" Research and Documentation Centre 64

9. Publications 67
9.1. Security and Personal Data Protection 69
9.2. Reviews 70
9.2.1. Spanish Data Protection Review 70
9.2.2. Digital Review www.datospersonales.org 71
9.2.3. Digital Review www.dataprotectionreview.eu 72
9.3. Monographs on Data Protection 74
9.4. Sector Leaflets Containing Data Protection Information 74
9.5. Administrative Transparency and Personal Data Protection 75
9.6. Report of the 5th Edition of the Award for Best European Practices in Data Protection 76
10. Citizens Advice Service 77

11. Collaboration between the APDCM and other Control Authorities and Institutions 81
11.1. Inter-agency Working Group 83
11.1.1. Directors Working Group 83
11.1.2. Data Register Working Group 83
11.1.3. Inspection Working Group 84
11.1.4. Legal Analysis and Regulatory Working Group 85
11.2. Agreements and Collaborative Acts 85
11.2.1. Signed Agreements 85
11.2.2. Meetings with other Control Authorities 86
11.3. Conferences of the Director in Mexico, Argentina and Uruguay 86

12. International Activity 87
12.1. 31st International Data Protection Conference 89
12.2. EuroPriSe 89
12.3. Privacy Open Space (PrivacyOS) 90
12.4. PrimeLife 92
12.5. International Control Authority Conferences and Working Groups 92
12.5.1. Protection Data Authorities Spring Conference 92
12.5.2. Working Group for Dealing with European Union Complaints 93
12.5.3. Telecommunications Working Group 93
12.5.4. 8th Ibero-American Meeting 93
13. General Secretariat 95

Presentation

This report details the major courses of action taken by the APDCM in 2009 as part of a conscientious, professional and intense working environment, of which I would like to highlight the following:

As a Control Authority, the Agency processed 316 proceedings regarding inspection and rights protection, the latter showing a sharp increase that doubled the 2008 figure. Also becoming more frequent are requests for protection concerning the right to erase personal data appearing in Official Journals.

In 2009, as part of our inspection function, we continued the work begun the previous year to ensure compliance with the right to information regarding the collection of personal data via the web pages of the Town Councils in the Madrid Region.

Regarding the Personal Data File Register, the creation of files remained stable, although after the approval of Royal Decree 1720/2007, of 21 December, which set forth the Implementation Provision of the LOPD, erasures were made as well as rectifications in order to adapt the files to the said regulation.

With the approval of the Instructions on the personal data processing of newborn babies in health centres forming part of the Madrid Region single public health network, and on the processing of personal data when issuing medical certificates in such centres, personal data processing was adapted to both data protection and sector legislation.

In the context of minors' rights to protection of privacy, the APDCM drew up the *Personal Data Protection Information Plan for School Children*. As part of the plan an information session was held in each of the 404 Secondary Schools in the Madrid Region on 28 January 2009, so that it would coincide with European Data Protection Day. The event was widely covered by the different media.

As part of the work to provide consultancy and help to file controllers, we can highlight several specific plans. In the context of security, the APDCM requested an audit to be made of all medium and low level files. We also ensured that file controllers were properly adapting their processing to the legislation approved in recent years by the APDCM. This specifically referred to the instructions and recommendations concerning the publication of personal data on the Internet and in Official Electronic Journals, personal data processing in e-Government services and personal data processing using video cameras.

PRESENTATION

In order to educate people in the data protection culture and promote it, a handbook on *Security and Data Protection* was published, following the line begun in 2008, in which year various sector handbooks were published, building an even more solid foundation for the periodic publications of the APDCM, www.datospersonales.org, www.dataprotectionreview.eu and the Spanish Data Protection Review.

Data protection leaflets were also prepared for the health and social services sectors, which were sent to the relevant welfare centres for distribution.

Four specific conferences were also held, participated not only by the APDCM but also by file controllers who had the chance to contribute their experience: 4th Schools Conference, 2nd Security Conference, 2nd Local Police Conference and the Guidance Teams Conference.

Regarding the use of information technologies, the APDCM changed its institutional portal in 2009, giving it a much more attractive design for easier navigation. A virtual data protection training tool was also launched in collaboration with ICM. This tool received 1289 applications from public employees to enrol on the online course.

Finally, I would not want to end without thanking all the hard work and effort put in by APDCM staff and my predecessor in the post, Mr Antonio Troncoso Reigada, without whom the presentation of this Activities Report would not have been possible.

Santiago Abascal Conde
Director of the APDCM

1. Data Register

1. Data Register

1. DATA REGISTER

Act 8/2001, of 13 July on Data Protection in the Madrid Region sets out in article 18 that the Data Protection Agency of the Madrid Regional Government shall keep a register of Personal Data Files. This register has a dual purpose: to enable individuals to exercise their rights in respect of any data processing carried out by public institutions within the Madrid Region and serve as a tool to ensure compliance by other units and bodies of the Agency.

The Register of Personal Data Files shall contain the personal data files owned by the Madrid Regional Government Institutions and by the Bodies, Agencies, Public Corporations and other Local Authorities forming part of its Public Administration with the exception of commercial companies. The file shall also contain personal data files created or managed by the Authorities forming part of the Local Administration of the Madrid Regional Government, in compliance with the provisions of the articles of Act 41 15/1999, of 13 December as well as the files created or managed by the Public Universities and Local Authorities representing the economic and professional interests of the Madrid Region, provided, in the latter case, that the said files are created or managed for the purpose of exercising public powers.

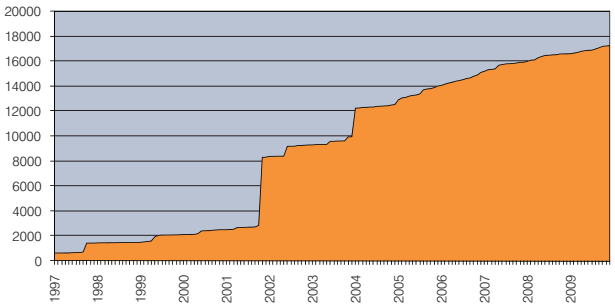
Consultation of the Data Register is free-of-charge and is available to any person who requests such, particularly via the Internet at the web site of the Agency, *www.apdcm.es*, on the "Data Register" channel.

As set forth in Article 20.2 of Act 8/2001, the Madrid Regional Government Data Protection Agency shall periodically submit the content of the Register of Personal Data Files to the Spanish Data Protection Agency with the purpose of its being entered in the General Data Protection Register.

The entry of new files done in 2009 revealed a steady growth trend in respect of previous years. The reason for this must be sought in the high level of file regularisation already existing in certain areas of competence of the Madrid Regional Government Data Protection Agency, particularly within its Administration. Since 2007, 100% of Professional Bodies have declared their files, and in the first six months of 2008, 100% of Town Councils within the Madrid Region had entered their files in the Register. This increase is also due to the growing number of video surveillance files as the APDCM is working with file controllers in order to regularise them.

1. DATA REGISTER

Chronological evolution of the TOTAL number of Registered Files



2009 also saw an increase in the number of files erased, which was justified by the application of article 2.2 of Royal Decree 1720/2007, of 21 December, governing the regulations developed in the LOPD, by virtue of which the the cited Regulation is not applicable either to any processing referring to corporate bodies or to any files that are limited to incorporating the data of any legal persons working for the said corporate bodies that only consist of their name and surname, the duties performed or the position held, including the postal or electronic address, and business telephone and fax numbers.

It should be pointed out that the different tables do not reflect any rectifications made to entries as a result of the changes to the organisational structure of the different Departments of the Madrid Regional Government. The Madrid Regional Government only adapts entries periodically, an undertaking that means 8,000 entries being rectified for each structural change carried out.

In this respect, these rectifications are made officially by the APDCM in accordance with the rules set forth in the First Additional Provision of Decree 99/2002, of 13 June, which regulates the procedure for drawing up general requirements for the creation, rectification and erasure of files containing personal data as well as their entry in the Personal Data Files Register, with the approved Decree on structure being the basis of the general regulations governing any rectifications required to the said Register.

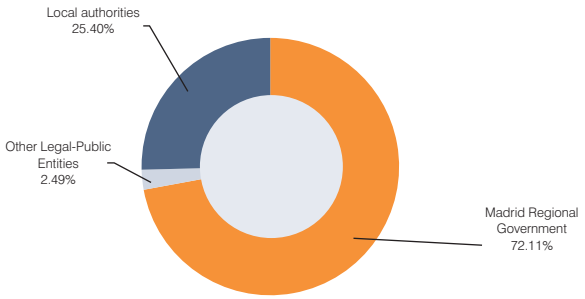
INDICATOR	REGISTERED FILES (ONLY ACTIVE ONES)						
	2005	2006	2007	2008	2009	Variation	
Madrid Regional Government	11,311	11,390	11,727	11,959	9,905	-2,054	-17.18%
Other Legal–Public Entities	237	278	310	323	342	19	5.88%
Local Authorities	1,621	2,530	2,884	3,244	3,489	245	7.55%
TOTAL	**13,169**	**14,198**	**14,921**	**15,526**	**13,736**	**-1,790**	**-11.53%**

INDICATOR	REGISTERED FILES (INCLUDING ERASURES AND TEMPORARY FILES)						
	2005	2006	2007	2008	2009	Variation	
Madrid Regional Government	11,311	11,982	12,508	12,792	12,988	196	1.53%
Other Legal-Public Entities	237	288	326	350	379	29	8.29%
Local Authorities	1,621	2,691	3,088	3,498	3,881	383	10.95%
TOTAL	**13,169**	**14,961**	**15,922**	**16,640**	**17,248**	**608**	**3.82%**

Adapting file entries to new Departmental structure provides individuals with an effective way of identifying the ownership of the data processed by the Madrid Regional Government and, above all, enables them to exercise their rights as set forth in Data Protection regulations before the body that is actually responsible for processing their data.

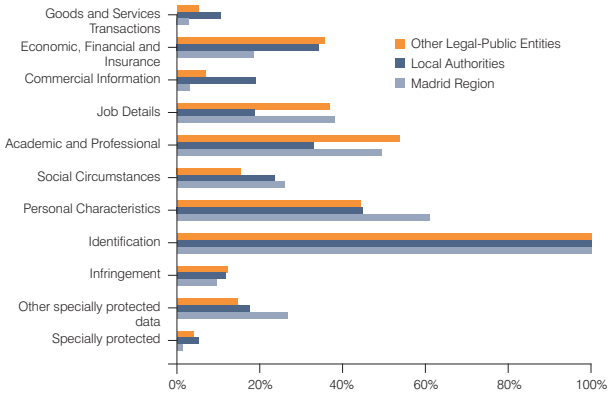
Another considerable number of file rectification entries (over 4000) were made to adapt the level of security entered in those manually created files to which the specifications set forth in Royal Decree 1720/2007 of 21 December were applied.

Registered Files by Administration Type (31/12/2009)



Regarding the classification of the Data Register according to data type, apart from the data on identification that all files must contain, it can be seen that most files correspond to academic and professional data as well as personal data.

Average number of Registered Files according to Data type



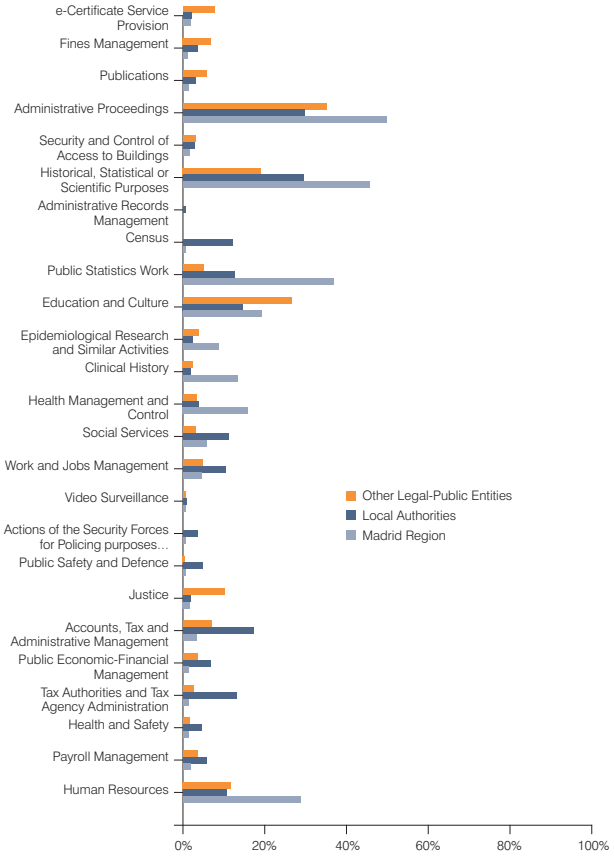
Regarding the purpose of these files, since the Public Administrations are service providers, the purpose of almost 50% of the files entered was to carry out administrative procedures.

REGISTERED FILES ACCORDING TO DATA TYPE	MADRID REGIONAL GOVERNMENT		LOCAL AUTHORITIES		OTHER LEGAL-PUBLIC ENTITIES		TOTAL	
	Files	%	Files	%	Files	%	Files	%
Specially protected	168	1.29%	202	5.20%	15	3.96%	**385**	**2.23%**
Other specially protected data	3,460	26.64%	673	17.34%	55	14.51%	**4,188**	**24.28%**
Infringements	1,232	9.49%	452	11.65%	46	12.14%	**1,730**	**10.03%**
Identification	12,988	100.00%	3,881	100.00%	379	100.00%	**17,248**	**100.00%**
Personal data	7,939	61.13%	1,741	44.86%	168	44.33%	**9,848**	**57.10%**
Social circumstances	3,394	26.13%	911	23.47%	58	15.30%	**4,363**	**25.30%**
Academic and professional	6,390	49.20%	1,273	32.80%	204	53.83%	**7,867**	**45.61%**
Job details	4,935	38.00%	718	18.50%	139	36.68%	**5,792**	**33.58%**
Commercial information	399	3.07%	731	18.84%	25	6.60%	**1,155**	**6.70%**
Economic, financial and insurance	2,374	18.28%	1,328	34.22%	135	35.62%	**3,837**	**22.25%**
Goods and services transactions	371	2.86%	400	10.31%	19	5.01%	**790**	**4.58%**

1. DATA REGISTER

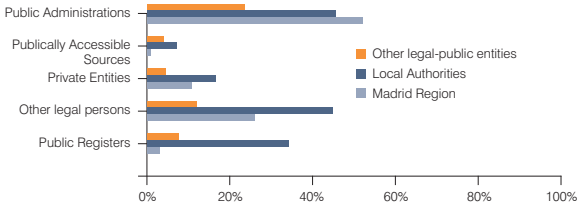
FILES REGISTERED ACCORDING TO PURPOSE	MADRID REGION		LOCAL AUTHORITIES		OTHER LEGAL-PUBLIC ENTITIES		TOTAL	
	Files	%	Files	%	Files	%	Files	%
Human Resources	3,685	28.37%	408	10.51%	44	11.61%	**4,137**	**23.99%**
Payroll Management	199	1.53%	206	5.31%	12	3.17%	**417**	**2.42%**
Health and Safety	101	0.78%	156	4.02%	5	1.32%	**262**	**1.52%**
Tax Authorities and Tax Agency Administration	133	1.02%	500	12.88%	9	2.37%	**642**	**3.72%**
Public Economic-Financial Management	131	1.01%	244	6.29%	12	3.17%	**387**	**2.24%**
Accounts, Tax and Administrative Management	394	3.03%	661	17.03%	25	6.60%	**1,080**	**6.26%**
Justice	192	1.48%	56	1.44%	37	9.76%	**285**	**1.65%**
Public Safety and Defence	29	0.22%	169	4.35%	1	0.26%	**199**	**1.15%**
Actions of the Security Forces for policing purposes	12	0.09%	123	3.17%	0	0.00%	**135**	**0.78%**
Video Surveillance	33	0.25%	12	0.31%	1	0.26%	**46**	**0.27%**
Work and Jobs Management	521	4.01%	386	9.95%	17	4.49%	**924**	**5.36%**
Social Services	681	5.24%	420	10.82%	10	2.64%	**1,111**	**6.44%**
Health management and control	2,025	15.59%	141	3.63%	11	2.90%	**2,177**	**12.62%**
Clinical history	1,680	12.94%	63	1.62%	8	2.11%	**1,751**	**10.15%**
Epidemiological Research and similar activities	1,109	8.54%	73	1.88%	13	3.43%	**1,195**	**6.93%**
Education and Culture	2,437	18.76%	558	14.38%	100	26.39%	**3,095**	**17.94%**
Public Statistics Work	4,780	36.80%	483	12.45%	17	4.49%	**5,280**	**30.61%**
Inhabitants Register	32	0.25%	454	11.70%	0	0.00%	**486**	**2.82%**
Promotional Census Management	0	0.00%	6	0.15%	0	0.00%	**6**	**0.03%**
Historical, Statistical or Scientific Purposes	5,880	45.27%	1,126	29.01%	71	18.73%	**7,077**	**41.03%**
Security and control of access to buildings	163	1.26%	47	1.21%	10	2.64%	**220**	**1.28%**
Administrative Proceedings	6,438	49.57%	1,143	29.45%	132	34.83%	**7,713**	**44.72%**
Publications	130	1.00%	51	1.31%	20	5.28%	**201**	**1.17%**
Fines management	117	0.90%	125	3.22%	25	6.60%	**267**	**1.55%**
e-Certificate Service Provision	188	1.45%	68	1.75%	28	7.39%	**284**	**1.65%**

Average Number of Registered Files According to Purpose



Finally, regarding data sources and bearing in mind the explanation given in the aforementioned statistics, over 50% of data come from the cited Public Administrations.

Average Number of Registered Files according to Data Source



FILES REGISTERED ACCORDING TO DATA SOURCE	MADRID REGION		LOCAL AUTHORITIES		OTHER LEGAL–PUBLIC-ENTITIES		TOTAL	
	Files	%	Files	%	Files	%	Files	%
Public Registers	406	3.13%	1,322	34.06%	30	7.92%	**1,758**	**10.19%**
Other legal persons	3,386	26.07%	1,739	44.81%	46	12.14%	**5,171**	**29.98%**
Private Entities	1,421	10.94%	650	16.75%	17	4.49%	**2,088**	**12.11%**
Publically Accessible Sources	124	0.95%	282	7.27%	16	4.22%	**422**	**2.45%**
Public Administrations	6,762	52.06%	1,768	45.56%	89	23.48%	**8,619**	**49.97%**

2. Control of Files. Protection of Rights and Inspection

2. Control of Files. Protection of Rights and Inspection

2. CONTROL OF FILES. PROTECTION OF RIGHTS AND INSPECTION

2.1. ADMINISTRATIVE PROCEDURES

2.1.1. Introduction

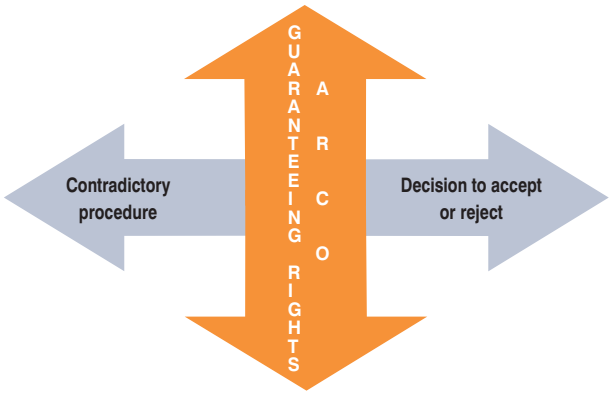
The Sub-directorate of Inspection and Protection of Rights is the administrative unit of the APDCM that is responsible for exercising the duties deriving from the powers of inspection, which duties are governed by article 19 of Act 8/2001 of 13 July.

Therefore, this administrative unit is responsible for driving and investigating the proceedings brought about by the complaints and claims lodged by individuals in order to protect their rights of access, rectification, erasure and opposition, in addition to the proceedings for infringement against the Public Administrations that are opened as a result of the control mechanisms carried out to determine whether or not there is any infringement of what is envisaged in the LOPD.

2.1.2. Rights protection

The administrative proceedings for the protection of rights are always opened as the result of a complaint filed by an individual when they consider that their rights of access, rectification, erasure and opposition have not been properly addressed by the data controller.

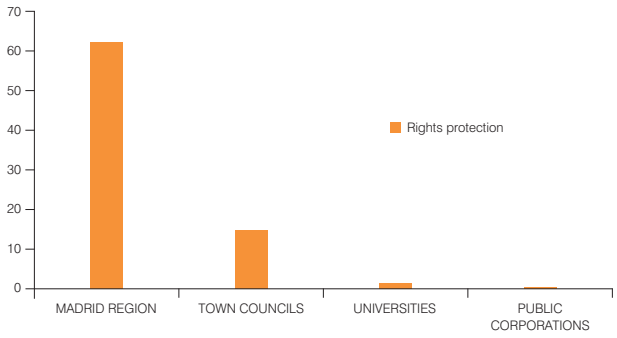
These proceedings are regulated by Decree 67/2003, of 22 May. These proceedings are distinguished by their contradictory nature, insomuch as both the data controller and the individual can make allegations in their defence. The decision of the APDCM shall be accepted if the right of access, rectification, opposition or erasure has not been duly dealt with, or rejected, if the contrary is the case.



As in previous years, there has been a continuous growth in rights protection proceedings. If 54 claims were filed in 2008 concerning the exercise of ARCO (Access, Rectification, Cancellation, Objection) rights, in 2009 this number practically doubled, with a total of 101 complaints.

This progressive increase is due to two circumstances: firstly, the Data Protection Control Authorities, obviously including the APDCM, are supervising the exercise of ARCO rights with regard to clinical histories. In this respect, in 2009, 25 claims were received from individuals concerning the exercise of

ARCO rights over the files in the possession of the Health Department. Most of these claims were requests for access to, or erasure of clinical histories. Secondly, claims filed to request the protection for the right of erasure concerning the data published in official journals and gazettes have become more frequent.



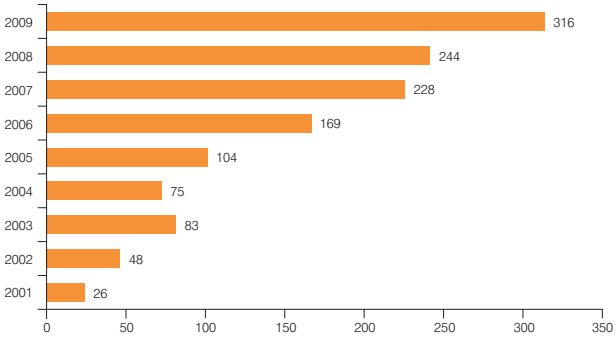
2.1.3. Inspection Proceedings

Opening inspection proceedings is always ex-officio even if the said initiative is motivated by an individual's complaint. The APDCM also opens these kinds of proceedings through several channels: through the initiation of an inspection plan, through the appearance of some news in the press which might be an infringement of data protection, or when there is evidence from other sources of a possible infringement of data protection regulations.

As with the protection of rights, inspection proceedings are also regulated by Decree 67/2002, of 22 May. Apart from regulating inspection itself, it also regulates the infringement proceedings in the event of there being indications that data protection was violated by actions undertaken by the data controller.

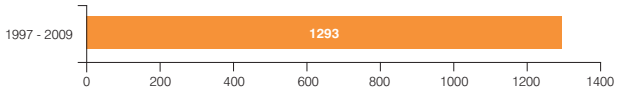
If we referred to a noticeable increase in the number of inspection proceedings, including rights protection, in the 2008 Report, in 2009 a total of 316 protection proceedings were opened. Unlike in 2008, when the number of proceedings was largely due to the inspection plans implemented by the APDCM, in 2009 the increase was basically due to individuals filing claims.

Cases processed
Control and rights protection function



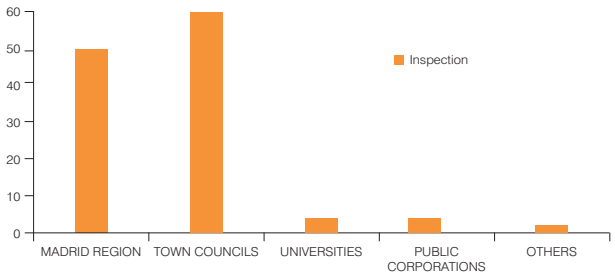
In this respect, it should be emphasised that since the APDCM was set up, over one thousand inspection and rights protection proceedings have been dealt with.

Cases processed
Control and rights protection function

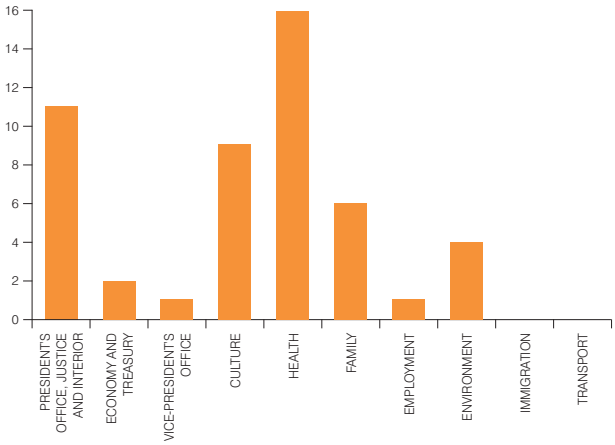


Of the 316 proceedings dealt with, we need to discern those corresponding to inspection duties and those corresponding to rights protection duties.

Regarding the former, 215 proceedings have been dealt with, fifty corresponding to the Administration of the Madrid Regional Government, sixty to Local Authorities, four to Universities, four to Public Corporations and two to other Public Institutions. Moreover, 62 were the responsibility of the Spanish Data Protection Agency.



Regarding the inspection proceedings opened against Madrid Regional Government bodies, sixteen corresponded to the Department of Health, nine to the Department of Education, eleven to the President's Office, Justice and Interior, six to the Department of the Family and Social Affairs, four to the Department of the Environment, Housing and Town and Country Planning, two to the Department of the Economy and Treasury, one to the Department of Employment and Women, and another to the Vice-President's Office, the Department of Culture and Sports and the Government Spokesperson's Office.



In 2009 thirteen decisions were issued – in 2008 eight were issued- due to the data controller failing to comply with some of the principles of the LOPD. Some of these principles are listed below:

- Decision for infringement against a Health Centre for not having any security measures in place.
- Decision for infringement against a Town Council for violating the principle of quality in the use of a digital signature.
- Decision for infringement against a Town Council for not having an individual's file properly updated.
- Decision for infringement against a Health Centre for disclosing personal data without consent or for contravening some of the circumstances covered by art. 11.2 of the LOPD.

Finally, the APDCM publishes the rulings of its inspection and rights protection proceedings completely anonymously, in its institutional web *(www.apdcm.es)*, thereby complying with its principles of administrative transparency.

2.2. INSPECTION PLANS

2.2.1. Introduction

Article 18 of Decree 67/2003, of 22 May governing the Implementation Provision for the functions of the APDCM to protect rights and control personal data files, also regulates the Sector Inspection Plans, as one of the APDCM's control functions.

These preventive plans consist in examining each sector of activity of the public administration whose files are subject to Act 8/2001, of 13 July to determine the extent to which the said files comply with data protection principles and to ensure that public data controllers enforce compliance with the rights of access, rectification, erasure and opposition that may be exercised by individuals.

When the inspectors have examined all the information and completed the necessary actions and verifications, the Director of the APDCM will issue, in accordance with article 15.d) of Act 8/2001, of 13 July, the precise instructions, where it will be determined if the public files subjected to the sector plan are adapted or not to data protection regulations.

2.2.2. 2008-2010 Inspection Plan on compliance with data protection regulations when collecting the said data via the web pages of the Town Councils of the Madrid Region

In 2008 the APDCM implemented this Inspection Plan in order to know the degree of compliance with Recommendation 3/2008, of 30 April of the APDCM, on personal data processing in e-Government services (see sub-section 3.4 of the 2008 Report).

Within the framework of Local Government and in recognition of the right of individuals to communicate with the administration through electronic means (Act 11/2007, of 22 June, on the Electronic Access of individuals to the Public Services), numerous Town Councils of the Madrid Regional Government, taking advantage of the surge in technologies, have put different web pages into service so that individuals can carry out administrative procedures.

Although this Inspection Plan was designed to be implemented in the 2008-2009 period, after the approval of various regulatory standards comprising the said Act, the APDCM deemed it appropriate to extend the term of its implementation to the year 2010.

In this regard, and as we pointed out in the 2008 Report (see section 2.2.2), once all the investigative measures have been taken, an Individual Instruction will be sent to every Town Council for it to adapt its personal data collected through its web page, to data protection regulations, and particularly to the rules set forth in article 5 of the LOPD, as well as a General Instruction directed to all Town Councils, both those that have been inspected and those that have not, and which may be of use to other data controllers that are subject to the control functions of the APDCM.

3. Regulatory Development

3. Regulatory Development

3. REGULATORY DEVELOPMENT

3.1. INTRODUCTION

Article 6 of Decree 40/2004, of 18 March, on which the Statute of the APDCM is based, regulates regulatory development so that the APDCM can issue instructions and recommendations within its areas of competence to adapt personal data processing to the principles of the legislation in force in questions of data protection.

In this respect, following the line begun several years ago which led to the approval of Recommendation 1/2008, of 14 April on personal data processing in the Social Services of the Madrid Region and in the Social Services of the Local Authorities of the Madrid Region (*BOCM* of 7 May 2008), Recommendation 2/2008, of 25 April on the publication of personal data in official journals and gazettes on the Internet, institutional web sites and by other electronic and telematic means (*BOCM* of 8 September 2008), Recommendation 3/2008, of 25 April on the processing of personal data in e-Government services (*BOCM* of 11 September 2008), in 2009 the APDCM approved two new instructions, specially intended for data controllers in the health area.

3.2. INSTRUCTION 1/2009, OF 17 DECEMBER 2009, ON THE PERSONAL DATA PROCESSING OF NEWBORN BABIES IN THE HEALTH CENTRES FORMING PART OF THE SINGLE PUBLIC HEALTH SYSTEM OF THE MADRID REGION (BOCM OF 21 JANUARY 2010)

The ultimate purpose of the Instruction regarding the identification of newborn babies is to improve the fingerprinting system of the newborn child as well as their mother, so that they can be unmistakably identified and related, avoiding any confusion and problems arising from babies being mistakenly exchanged in health centres. A wrong identification of newborn babies makes a health service identity card meaningless and prevents a correct entry being made in the Civil Register.

Fingerprinting is a system that ensures that both are properly identified, as well as establishing the link between the newborn baby and its biological mother. Act 6/1995 of 28 March, which lays down the Guarantees of the Rights of Infants and Adolescents in the Madrid Region states that the most advanced and accurate methods available shall be used for data collection, to avoid any possible defects in the taking of fingerprints from causing the Identity Document to be lacking in validity.

Given the purpose of this data collection, such data shall not be able to be subject to erasure as it will continue to be necessary and relevant throughout the life of the newborn baby and its mother. Were the data figuring in the Mother-Child Health Identity Document to be stored in the clinical history, these shall not be the object of erasure or cancellation, even if the period for which the clinical history must be kept has expired, as set forth in Act 41/2002, of 14 November, the Regulatory Base regarding a Patient's Autonomy and Rights and Obligations in Matters of Information and Clinical Documentation.

3.3. INSTRUCTION 2/2009, OF 21 DECEMBER 2009, ON PERSONAL DATA PROCESSING IN THE ISSUE OF SICK LEAVE CERTIFICATES. (BOCM OF 21 JANUARY 2010)

This Instruction insists on the fact that there should be no requirement to provide personnel departments with more data than that which is strictly necessary to justify an absence from work, in order to prevent the diagnosis or the specific cause of the worker's illness from becoming known, as is already set forth in the regulations governing the issue of sick leave certificates.

Although a sick leave certificate is not required in the event of absence from work due to a common illness or non-work-related accident, the worker must justify their absence from work. Therefore, health centres must give the patient a document justifying attendance or the service provided.

One specific aspect regulated in this Instruction is to distinguish whether the person requesting the certificate is the sick worker themselves or any other member of their family, in which case the clear consent of the sick person or health centre user is required.

In addition, specific proceedings must be drawn up for this data processing, avoiding the use of documents prepared for health management –like the appointment form- as a justification, as this may refer to the health problem that may exist or the diagnostic test performed on the patient.

4. Assessment

4. Assessment

4. ASSESSMENT

As part of the assessment activity carried out by writing reports, four types can be distinguished:

- Mandatory reports on the creation, rectification and erasure of files.
- Reports on the adaptation of contracts and agreements to article 12 of the LOPD (processors).
- Mandatory reports for the approval of regulations.
- Reports that address the consultations made by data controllers.

The first on the list are in response to an obligation required by Act 8/2001, of 13 July on Personal Data Protection in the Madrid Region, which states that prior to the approval of general regulations for creating, amending or erasing a file, the proposal together with any allegations, must be sent to the APDCM for its mandatory report. Through this mandatory report, and having previously examined all the documentation sent, the APDCM carries out a "Prior Checking" activity, that is, a prior check on the legality of the personal data processing that is wished to be performed. Therefore, in 2009, 145 mandatory reports of this kind were compiled.

INDICATOR	2007	2008	2009
General file provisions published	121	160	136
Files regulated by published provisions	1,150	828	6,906

In respect of the reports on the adaptation of contracts and agreements to article 12 of the LOPD (processors), in accordance with this article, when processing is carried out by third parties, there must be a contract or agreement that stipulates the obligations with which the processor must comply regarding personal data.

In this respect, and in anticipation of their signing or processing, the APDCM has produced reports on 143 (in 2008 there were 132) agreements and contracts in relation to their being adapted to article 12 of the LOPD.

REPORTS ON CONTRACTS AND AGREEMENTS OF ARTICLE 12 OF THE LOPD	
Vice-President's Office, Department of Culture and Sport and Government Spokesperson's Office	3
President's Office, Justice and Interior	24
Department of the Economy and Treasury	7
Department of the Environment and Town and Country Planning	1
Department of Health	48
Department of the Family and Social Affairs	4
Department of Employment and Women	34
Local Authorities	21
Universities	1
TOTAL	**143**

4. ASSESSMENT

Regarding Mandatory Reports for the approval of regulations, during 2009 the APDCM produced mandatory reports for a total of 210 regulations, which is an increase of 53% compared to 2008, which reported 137 rules. Of these, the following are worthy of mention:

- Decree authorising Madrid Movilidad, S. A. to use remote capture resources through photographs, digital filming and other technology media, for their transfer to government agents.
- Decree by the Madrid Regional Government Council regulating the proceedings for appointing emeritus personnel to the Madrid Health Service.
- Royal Decree approving the minimum data set for clinical reports in the National Health System.
- Report by the Constitutional Affairs Committee for European Governance and Common Space of Freedom and Security and Justice of the Committee for the Regions, "The Stockholm Programme: challenges and opportunities for a new multiannual programme of the Common Space of Freedom, Security and Justice of the European Union".
- Government Council Decree regulating the exercise of the freedom of choice of family doctor, paediatrician and nurse in primary and hospital care and choice of doctor in specialist care.
- Madrid Regional Government Council Decree regulating the electronic edition of the *Madrid Regional Government Official Journal*.
- Decree to simplify the proceedings for authorisation and registration of Health Centres, Services and Establishments in the Madrid Region.

As has been the case for many years, the APDCM has also made reports on calls to apply for subsidies, among which the following should be mentioned:

- Decree laying down the regulatory base for granting financial aid in the form of a single payment for the birth or adoption of the third child or successive children to families of the Madrid Region and approving the 2009 call for applications.
- Decree governing the regulatory base for promoting technological innovation in the automotive sector of the Madrid Region, inviting calls for application for subsidies for 2009.
- Decree establishing the Emergency Financial Fund for Victims of Gender Violence in the Madrid Region, regulating the aid that can be granted from the said fund.
- Government Council Agreement "governing the regulatory standards and laying down the proceedings for directly granting single payment financial aid to families in the Madrid Region".
- Decree governing the regulatory base and calling for ap plications for subsidies intended for municipalities in the Madrid Region for the provision of a House Rental Service for Young People and a Young People's Mortgage.

Finally, regarding the Reports addressing the queries raised by data controllers, the replies to queries are contained in the Reports. These queries are related to issues concerning the transfer of personal data and the adaptation of personal data processing to the LOPD. While in 2008, 73 queries raised by the said controllers were addressed, in 2009, 98 were addressed, which is an increase of 34%.

The most marked queries addressed by the APDCM in 2009 were the following:

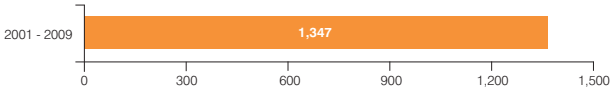
- Delivery of reports to a Health Insurance Company on the assistance given by the Local Police and the municipal ambulance in the workplace of a female council employee who subsequently died.
- Granting family members the right of access to the job sick leave files of a deceased person.
- Transfer of data contained in a "Residence Register of Spanish Citizens" and in a "Residence Register of Foreign Persons", requested by a town's Civil Guard Headquarters.
- Transfer of data contained in health reports on two minors being cared for by an association due to their continuous absences from school.
- Allowing a University Library to implement a text message service to inform students that the period for returning the books on loan had been exceeded.
- Allowing the Town Council to use data from the Municipal Census to wish the residents of the town a "happy birthday".
- Transfer of data on staff absenteeism to trade union representatives.
- What is meant by the data term "conscientious objector".
- Using a fingerprint-based access control to a Municipal Sports Centre in relation to a three year old girl who went to the Centre to take part in a "body movement" class.
- The response of the Madrid Region Free Legal Aid Committee regarding requests of access to the free legal files of the judicial proceedings referring to the right to free legal aid by both the opposing parties of the legal proceedings and the professionals designated to such proceedings.
- Timetable control file using staff fingerprints in a Madrid Region Secondary School.
- Access to the identity of the biological mother of a person (there was no proof of identity or reference to her being a minor or of legal age in the consultation) born in a hospital who was handed over in adoption and whose information is not on their birth certificate.
- Proceedings and contents of the medical certificates issued by health centres of the Madrid Region single health network.
- Various issues related to whether or not, in accordance with what is set out in data protection regulations, the processing and transfer of personal data can be undertaken regarding the victims of abuse or violent intra-family circumstances.
- Allowing the erasure from a first cycle Primary Education pupil's file of any reference to the special remedial classes received concerning "Therapeutic Educational Psychology and Speech Therapy" given to the said pupil and the reports issued in respect of the minor.
- The need to create a new personal data as a consequence of the "electronic edition" of the *Madrid Regional Government Official Journal*, which will start publication on the 2 January 2010.
- An analysis of the access to information contained in the e-mail accounts of public employees who work for the City Council.

4. ASSESSMENT

PUBLIC ADMINISTRATION	REGULATIONS	TRANSFERS	ADAPTATION LOPD	TOTAL
First Vice-President's Office	2	1	1	4
President's Office, Justice and Interior	15	2	3	20
Economy and Treasury	17	0	0	17
Transport and Infrastructures	0	0	0	0
Education	28	5	4	37
Environment and Housing	36	1	1	38
Health	14	17	8	39
Culture, Sports and Tourism	1	0	0	1
Family and Social Affairs	21	1	2	24
Employment and Women	65	1	1	67
Immigration and Cooperation	9	0	0	9
Independent Organisations	0	0	1	1
Other Institutions	0	2	4	6
Town Councils	2	20	11	33
Professional Associations	0	2	5	7
Universities	0	4	1	5
Total	**210**	**56**	**42**	**308**

In all, in the period between 2001 and 2009, the APDCM prepared over 1300 legal reports on the regulatory issues and queries raised by data controllers.

Legal Reports On Provisions and Queries



5. Consultation

5. Consultation

5. CONSULTATION

Regarding Consultation, the duties of the Subdirectorate General for Consultancy and Data Registration in its Consultancy aspect are to assess data controllers as to the best way to implement the measures needed to meet data protection regulations and adapt processing to these regulations to safeguard individuals' rights.

In order to fulfil these requirements the figure of the "Data Protection Coordinator" is essential. This is a person designated to each of the data controllers supervised by the Agency whose job is to make dialogue more effective and who can inform the APDCM of their problems and queries as well as informing the whole organisation about Agency criteria and the proposed solutions. This person carries out duties similar to those which in European Institutions are performed under the name of *"Data Protection Officer"*.

The annual planning of the APDCM sets out the actions to be developed in the course of the year by each data controller in the different areas of assessment, of which some of the most important are the following:

- creation, rectification and erasure of files;
- regularisation of existing files;
- training public employees;
- compliance with article 5 of the LOPD (right to information);
- compliance with article 12 of the LOPD (processor);
- adoption of security measures and security document;
- dissemination of instructions and recommendations approved by the APDCM.

Likewise, as part of the 2009 programme, the various training workshops held are worthy of mention. Particularly important were those devoted to training the officers from the Local Police Forces of the Madrid Region and training in personal data processing security, both of which were well-attended. Also, during this last workshop, those attending were given the Madrid Data Protection Agency's publication entitled "Security and Personal Data Protection", where file controllers can find the information and guidelines they need to implement a security policy that puts into practice the legal precepts of the Implementation Provision of the LOPD.

Finally, the initiative set into motion by the APDCM to raise awareness among Secondary pupils in the Madrid Region concerning the risks to their privacy existing in the Internet and particularly in social networks was highly significant and had a major social impact. Due to its importance, this initiative is described in detail in section 6 of this Report.

5.1. SECTOR PLANS

5.1.1. Video Surveillance

The installation of image capture systems through video surveillance has seen exponential growth in recent years. As a result, the personal data processing of images captured by these devices is becoming more and more commonplace, and because of its special nature it does not fit into the traditional concept of a file. The APDCM has therefore deemed it necessary to publish an instruction to clarify the situation and precisely define the obligations of the organisations that use these video surveillance systems.

For this reason, in 2007, the APDCM drew up and approved Instruction 1/2007, of 16 May, on personal data processing by means of camera or video camera systems in the area of the Madrid Regional Government Authorities and Public Administrations with the purpose of regulating and adapting these systems to the requisites of the right to personal data protection by making more rational and ordered the capture, recording, storage, manipulation, blocking, erasure and transfer of images of natural persons carried out by the Authorities and Public Administrations of the Madrid Regional Government.

Before installing a video surveillance system, the data controller must assess if it is possible to use a less intrusive system than video surveillance, and should it be decided to install it, they must justify in a report to the APDCM the need and fitness of purpose of installing video surveillance cameras. Subsequently, general regulations will have to be drawn up and approved to create a file. Notices will need to be put in place to notify that the zone is under video surveillance in conformity with article 5 of the LOPD and a procedure set to facilitate the rights of access, opposition and erasure exercised by the interested parties and ensure the erasure of any video recordings once a maximum of 30 days have passed since capture of the images.

Nº	THE 6 COMMANDMENTS OF VIDEO SURVEILLANCE
1	Evaluate whether a less obtrusive system can be used.
2	Draw up a report to justify the need and fitness of purpose of installing video surveillance.
3	Approve general regulations to create a file.
4	Put an information notice in place.
5	Do not use cameras in toilets or bathrooms.
6	Erase the images after a maximum of 30 days.

For these reasons, in 2008 the Subdirectorate General of Consultancy and File Registration embarked on an intense task to publicise the precepts of the Instruction, with the results referred to in the Report concerning this work. However, given the large number of video surveillance installations dealt with by public file controllers under the supervision of the APDCM, it was decided to continue encouraging these systems to be regularised throughout 2009 and particularly for files to be notified to the Personal Data File Register of the Madrid Regional Government and for

compliance with the obligation to inform through the required notices.

In the APDCM Personal Data File Register, a total of 88 video surveillance files were registered as of 31 December 2009, which are distributed as in the table below:

VIDEO SURVEILLANCE FILES ENTERED IN THE FILE REGISTER OF THE APDCM	
Town Councils	26
Economy and Treasury	7
Vice-President's Office and Government Spokesperson's Office	3
Education	7
Employment and Women	4
President's Office, Justice and Interior	6
Health	26
Transport and Infrastructures	3
Family and Social Affairs	1
Department of the Environment and Town and Country Planning	3
Universities	3
Total	**88**

Although, as already stated, major steps forward were made in 2008 in implementing Instruction 1/2007, some significant examples of the results achieved in 2009, which was the plan's second year of validity, will now be included.

Of these we can mention the declaration and review of video surveillance systems, which, in the interests of ensuring the safety of people and objects, were installed at the headquarters of the Vice-President's Office, Justice and Interior, the Department of Transport and Infrastructures, the Department of Employment and Women and the Department of the Environment, Housing and Town and Country Planning.

In the area of Social Services, we must underline the declaration of video surveillance files at the Reina Sofía Centre, many of whose residents are suffering from Alzheimer's. The installation is intended to protect them from threats as well as from any incidents that might arise as a consequence of their illness.

Within the health area, 2009 saw the completion of the procedures for the general regulations to create fifteen new video surveillance files. This is an increase of 136% compared to the files registered in the previous year. The new files correspond to the headquarters of Government Central Services and various hospitals, as well as the Madrid Medical Emergency Service (SUMMA 112) and the Madrid Region Transfusion Service.

The installation of video surveillance cameras in state schools and organisations belonging to the Department of Education has met with favourable reports in those cases where they were seen to meet the principles of fitness of purpose (adapted to the purpose proposed), need (the lack of any other methods to achieve the purpose) and proportionality (preponderance of major general interests to justify the restriction of individual rights).

For these verifications, mainly aspects like the following were taken into account: location of the state school (waste ground, isolated spots with few passers-by; recurrent conflict in the school; occasional incidents such as acts of vandalism, destruction of furniture and theft of teaching resources; entry into the school of outsiders or unauthorised persons during class time; the installation of cameras in places where they do not affect the rights and privacy of teachers and pupils or the pupils' rights to freely develop their personality. The number of cameras also had to be proportional to the area of the school grounds. In addition, the video surveillance systems installed

were declared and registered at the central headquarters of the Department of Education.

Regarding the Local Administration, most of the video surveillance processing declared corresponds to action by Local Police to keep the public buildings in their custody under surveillance or to improve public safety in conflictive areas. In all cases, justification was demanded for the need of such installation in strict observance of the principles of fitness of purpose, need and proportionality.

Of special interest is the file declaration of the video camera recordings of the courses, conferences and events, with the prior consent of the attendees, which take place in the Comprehensive Safety and Emergency Training Centre of Madrid City Council (CIFSE). This is an excellent tool for training emergency service personnel (fire-fighters, health workers, police, civil defence, etc).

In the area of Justice and Interior, worthy of mention is the completion of the proceedings for declaring video surveillance files for the purposes of security and control of the accesses to all the offices of Justice, State Prosecutors and other buildings housing the Madrid Regional Government Justice Administration Service, as well as the installations at the Madrid Region Fire Brigade Headquarters and at the centres of the Madrid Region Agency for the re-education and reinsertion of young offenders.

To complete this section, it must be underlined that during this year the Complutense University and the Autónoma University completed their proceedings to declare their respective video surveillance files concerning security and control of access to their buildings and facilities, which they regularised by the general regulations pursuant to each that were published in the *BOCM*.

5.1.2. SECURITY

5.1.2.1. Regularising security levels

With the entry into effect of the Implementation Provisions of Organic Act 15/1999, of 13 December on personal data protection, approved by Royal Decree 1720/2007, the security measures to be met by manual files containing personal data were set out and specified, thereby compensating the lack of Royal Decree 994/1999 of 11 of June in this area, which approves the Regulations regarding security measures for automated files containing personal data, since this latter Decree only set forth security measures for automated files.

As the new regulations set the same levels of security –minimum, medium and high- for manual files as for automated files, the obligation was also imposed to include the level corresponding to each on entry in the Personal Data File, as has always been the case with automated files.

Given the large volume of manual files in the Madrid Regional Government Personal Data File Register, it became necessary to design a plan with the participation of all the APDCM's consultants, in order to set in motion the approval proceedings for the general regulations required to assign the right level of security to these files, as well as for their subsequent entry in the Personal Data File Register.

As a result of this plan, throughout 2009, a total of 3 872 files were completely regularised, in the Madrid Regional Government Administration as well as in Town Councils and other Madrid Region Institutions. Below is the chart showing the distribution of file regularisation by file controllers.

FILE CONTROLLER	FILE
President's Office, Justice and Interior	54
Department of the Economy and Treasury	68
Department of Transport and Infrastructures	3
Department of Education	2,077
Department of the Environment and Town and Country Planning	81
Department of Health	1,519
Department of the Family and Social Affairs	6
Department of Employment and Women	2
Other Madrid Region Institutions	3
Total Madrid Region Institutions	**3,813**
Campo Real Town Council	4
El Molar Town Council	2
Gargantilla del Lozoya and Pinilla de Buitrago Town Council	2
Navarredonda and San Mamés Town Council	2
Valle Medio del Lozoya Association	1
Pelayos de la Presa Town Council	4
Manzanares el Real Town Council	1
Montejo de la Sierra Town Council	4
La Hiruela Town Council	3
Rivas-Vaciamadrid Town Council	4
Sevilla La Nueva Town Council	3
Villa del Prado Town Council	3
Alcalá de Henares Town Council	2
Mejorada del Campo Town Council	4
Parla Town Council	13
Total Town Councils	**52**
Madrid Polytechnic University	4
Madrid Autónoma University	2
Professional Association of Dental Hygienists of the Madrid Region	1
Total other legal-public entities	**7**
Total files regularised	**3,872**

5.1.2.2. Security Audits

Legislation regarding matters of personal data security lays down that file controllers are required to carry out twice yearly security audits in order to ensure that medium to high level security files and the information processing systems and the premises where they are located meet the required security measures.

In order to verify this requirement the Madrid Regional Government Data Agency sends a letter of formal notice to all file controllers entrusted with implementing medium and high level security measures, reminding them of the need to perform these audits and requesting them to submit the reports with the results of the audits to the Agency.

The last letter of notice was issued in November 2008 and the analysis of the results submitted that were sent to the APDCM throughout 2009 show that there have been significant improvements in all the areas audited compared to the audits reviewed in the previous year.

Analysing the results of the previous wave of audits was extremely complicated as the letter of notice did not state any rule requiring the audits to be done with any unified format or method. This made uniform processing of the information received very difficult.

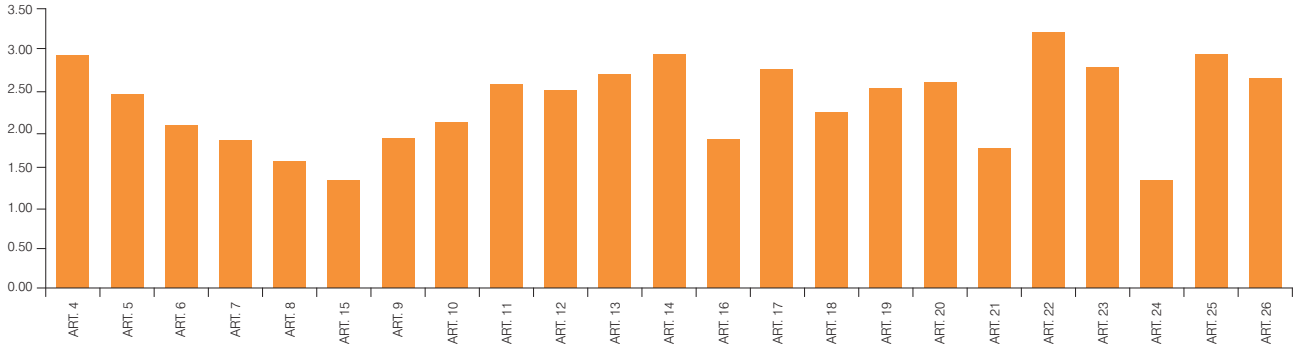
However, although the last letter of notice scrupulously recognised the autonomy of the auditors to apply the professionally recognised methodology they considered most appropriate, provided it verified every aspect specified in the Implementation Provision of the LOPD, they were requested to attach a unified summary of the results so that the information could be better processed and a more objective comparison be made of the data, which made it easier to analyse the information. The following table includes the different levels of evaluation used in this summary.

0	Zero. Total non-compliance
1	Very deficient compliance. Many serious deficiencies
2	Deficient compliance. Various deficiencies, some serious
3	Normal compliance. Without comment or with some non-serious deficiencies
4	Good compliance. Good comments with no reference to deficiencies
5	Excellent compliance. Very good comments

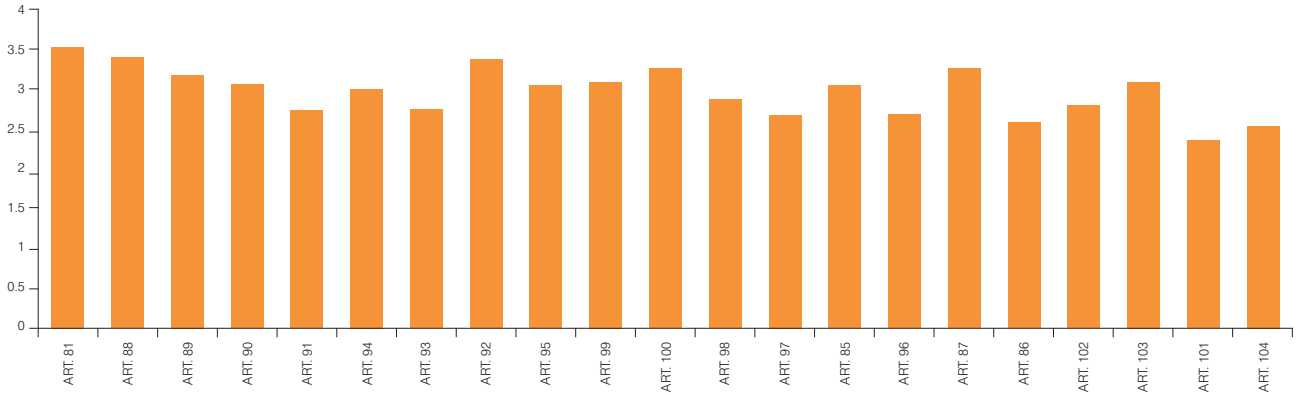
The outcomes of the audits were analysed to determine the degree of compliance with security measures by data controllers and those entrusted with this compliance in order to find the most habitual weak points and work to rectify them.

Included below are the graphs showing the results of the two waves of audits where the aforementioned improvement can be appreciated.

Results of the previous audit



Results of the 2009 audit



As can be seen, even bearing in mind the differences in the regulations in force, in general, the audits received in 2009 reveal a degree of compliance that is notably higher than on previous occasions. However, there are still important deficiencies concerning key issues, such as those regarding control of access and identification, support and document management and data encryption.

5.1.3. Publication of Personal data on the Internet and Official Electronic Journals

The electronic format publication of official journals and gazettes on the Internet has been a major step forward in the availability of information for a large number of people who did not have access to such when it was only published in hard copy. However, a consequence of this ease of access to information is the myriad of data on people that often describes very private aspects of their personal life (notifications of fine proceedings, handicaps, subsidies, etc). This is the result of the indexing of the content of official

journals and gazettes performed by different search engines, which makes it almost universally available in the public domain.

The APDCM is aware of this situation and after numerous complaints from individuals it approved Recommendation 2/2008 on the publication of personal data in official journals and gazettes on the Internet, on institutional websites and by other electronic and remote media, where the general application of the principles of data protection for personal data published on the Internet were systematically and consistently approached, as was the specifying of the different kinds of situations that entail the publication of personal data on institutional websites and particularly in official journals and gazettes.

One of the fundamental issues dealt with in the recommendation is the duty of file controllers to notify the institutions entrusted with managing the official journals and gazettes of any approved requests to erase personal data in order to then be able to block such data in the corresponding official journal or gazette.

To encourage implementation of the Recommendation, and most particularly of this highly relevant issue, the Madrid Regional Government Data Protection Agency had numerous meetings and contacts with the Regional Organisation, the *Madrid Regional Government Official Journal* and with the Madrid Regional Government Computing and Communications Agency in order to find technical solutions to block the data of any persons who had their right to erasure recognised so as to avoid their being indexed by search engines.

As a result of this work many people have had their data blocked who had requested such. They have thus seen a wish satisfied that had been the cause of deep anxiety and worry.

Finally, it should be pointed out that the Madrid Regional Government has shown sensitivity to this problem and the Government Council published Decree 2/2010 of 28 January, governing the e-edition of the *Madrid Regional Government Official Journal*, which introduced a series of guarantees to ensure the proper processing of personal data published in the *BOCM*.

Therefore, article 9 subjects the services provided via the data base of the *BOCM* to what is set forth in data protection legislation by stating that “the Madrid Regional Government Official Journal Independent Body shall offer a free data base at its electronic headquarters that enables the regulations and acts published in the digital edition of the OFFICIAL JOURNAL OF THE MADRID REGIONAL GOVERNMENT to be searched, recovered and printed, in accordance with what is set forth in personal data protection legislation”.

Likewise and more specifically, the Second Additional Regulation on personal data protection states that “within the scope of their respective competencies, personal data protection controllers must insert announcements in the electronic edition of the OFFICIAL JOURNAL OF THE MADRID REGIONAL GOVERNMENT to determine the purpose, content and use of the personal data published, as well as the possibility to block such data when it has ceased to be necessary or relevant for the purpose to which it had been published”. This not only establishes the mandatory and binding nature of the possibility to exercise the right of erasure by blocking data, but also obliges those responsible for ordering the pu-

blication of personal data to set the period of time during which the data must remain at the disposal of *BOCM* users and the moment when such data must be blocked.

The Madrid Regional Government Data Protection Agency will continue to work throughout the coming year with the *BOCM* Independent Body and with ICM to promote compliance with these precepts and the content of Recommendation 2/2008, by the implementation of the new digital version of the *BOCM* and the technical and organisational measures that are required.

5.1.4. e-Government in the Madrid Region

2009 saw the final impulse towards e-Government in the Madrid Region. A tremendous effort was made, coordinated and directed by the Directorate General of Service Quality and Citizen's Advice in order to meet the requirements of Act 11/2007 on the Electronic Access of Individuals to Public Services.

As part of this great project hundreds of proceedings were reviewed and reengineered, some of which were offered via electronic means and in other cases offered for the first time via remote channels, which has affected all the bodies and agencies in the Madrid Region.

The Madrid Regional Government Data Protection Agency has lent all its support to this project and has closely cooperated with the Directorate General of Service Quality and Citizen's Advice to take advantage of this opportunity to better adapt the electronic services offered by the Madrid Regional Government to data protection regulations.

Thus, a thorough review was performed to ensure that all electronic procedures collecting and processing personal data were associated with a file registered in the Madrid Region Personal Data File Register and that such entry would faithfully reflect the reality of the processing performed and be adapted to the requirements of the Implementation Provision of the LOPD.

In this way it has been possible to take the next step towards normalising the information clauses in the electronic forms so that they will refer to the right file and meet all the requirements set forth in article 5 of the LOPD, in such a way that any individuals who communicate electronically with the Madrid Regional Government will be able to submit their data with every assurance.

Similarly, all the electronic data collection forms let an individual choose to exercise their right either not to submit data that are already possessed by the Administration or to submit them directly by including the appropriate consent request boxes together with the right information so the individual can make a free and informed decision.

Finally, a mechanism was set into motion to enable an individual to take out a personalised subscription to information concerning Madrid Regional Government services. This, in every case, has the individual's consent, with the individual being able to withdraw such consent at any moment.

6. European Data Protection Day

6. European Data Protection Day

6. EUROPEAN DATA PROTECTION DAY

In 2009 the Madrid Regional Government Data Protection Agency prepared a *Personal Data Protection Information Plan for School Children,* specifically aimed at pupils in Secondary Education. The aim of this Plan was to make pupils aware of their fundamental right to personal data protection and explain the threat to their privacy posed by modern information and communication technologies and try to make the youngsters aware of the need to use such technologies responsibly.

This Plan, which had the backing of the Department of Education, was based on three points:

- Point 1: to train teaching staff about personal data protection from a practical point of view connected with their job as a teacher.
- Point 2: to try to get across to pupils the importance of observing across- the-board personal privacy in different subjects –Literature, History, Social Sciences, Mathematics and Technology, etc- as well as in the subject of Citizenship.
- Point 3: to hold an information session in Secondary Schools in the Madrid Region on the risks of information technologies.

This information session (Point 3) took place on 28 January 2009, to coincide with European Data Protection Day. The information session took place in the 404 Secondary Schools in the Madrid Region. A total of 80,000 pupils between the ages of 15 and 16 attended the sessions.

The information session was given by over 60 experts in matters of data protection (Magistrates, Judges, Lawyers and Legal Experts) and Madrid Regional Government Data Protection Agency staff (including administrative staff, who also took part in giving the sessions).

School counsellors, tutors and heads of studies collaborated to cover the remaining Secondary Schools.

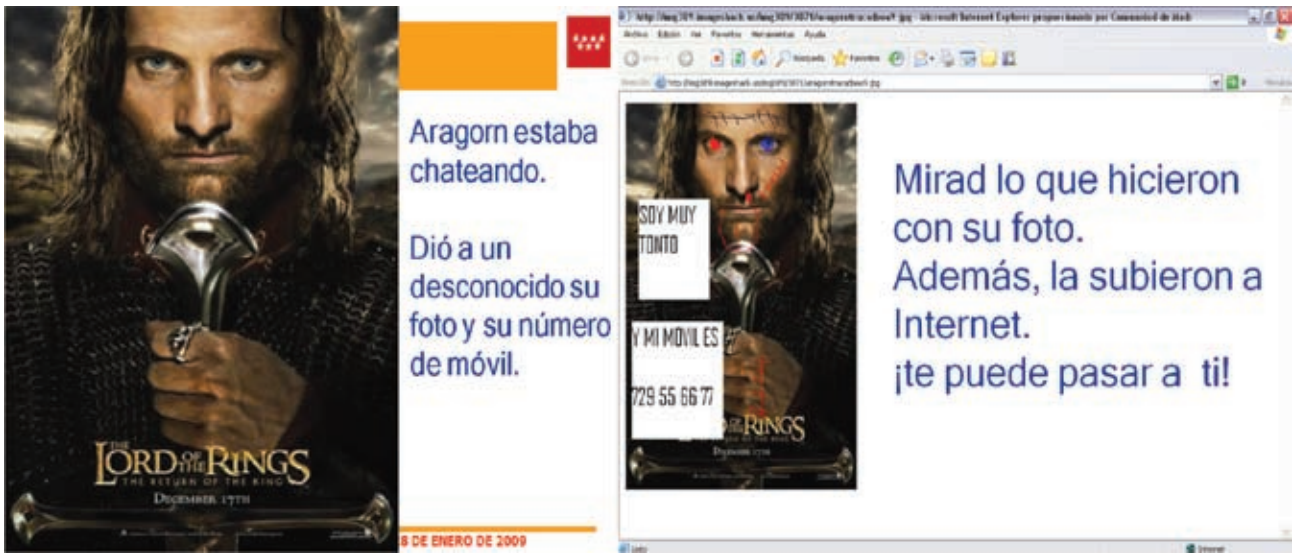
Prior to giving the information session Madrid Regional Government Data Protection Agency staff met the head teachers, heads of studies and counsellors of the Secondary Schools to provide them with the information required to give the information session. For this purpose, different preparatory meetings were held in the five educational areas of the Madrid Region (north, south, centre, east and west).

6. EUROPEAN DATA PROTECTION DAY

The purpose behind holding the information session on 28 January 2009 (European Data Protection Day) in the 404 Secondary Schools was to encourage a debate on the processing of the personal data that young people transmit every day through their use of social networks, instant messaging, chats, mobile phones, etc, and the present and future consequences of this, bearing in mind that no information disappears. Therefore, the session was structured as follows:

- The showing of six videos dealing with the problems of privacy in social networks, *cyber bullying*, thinking before publishing *(think before you post)*, how easy it is to post in the Internet and how difficult it is to erase opinions or photos from web pages ("Hotel California effect - you can check in any time you like, but you can never leave"), the mass publication of photographs or the fact that you never know who you are chatting to.
- A PowerPoint presentation illustrating examples of security, *spam*, the use of messaging *(messenger)* or the manipulation of photos.
- Handing out Data Protection Handbooks prepared by the Computer Freedom Committee non-governmental organisation. These Handbooks come in three different versions: for pupils from 9 to 11, from 12 to 14 and from 15 to 17. Through mime and colloquial language easily understood by the target audience, the various problems currently entailed by using the Internet are reflected, such as *cyber bullying*, *spam* or *phishing*.

This initiative made a large impact in the different social communication media, the printed press, the Internet and television.



Two of the PowerPoint slides.


"Piénsalo primero. Luego lo cuelgas"

El País Newspaper. 29/01/2009.

Information session in a Secondary School 28/01/2009.

The Campaign was presented at the European Conference in Edinburgh held in that city in April 2009 and at the meeting of the European Union Cross-Border Complaints Group *(Case Handling Workshop)* held in October 2009 in Limassol. In addition, the activities and outcomes of this campaign are to form part of a "White Paper" on these kinds of events organised by the European Data Protection Control Authorities that is being prepared by the Czech Republic Data Protection Agency.

Finally, the APDCM also held this information session with over 100 mothers and fathers of pupils, since these are the first who need to know the dangers that their children can come across when using these technologies.

7. e-Government

7. e-Government

7. E-GOVERNMENT

7.1. INTRODUCTION

Article 6 of Act 11/2007, of 22 June, on the Electronic Access of individuals to the Public Services, recognises the individual's right "to be able to communicate with Public Administrations by the use of electronic means in order to exercise the rights set forth in article 35 of Act 30/1992 of 26 November, as well as being able to obtain information, make consultations and allegations, make applications, express consent, file claims, effect payments, carry out transactions and object to administrative decisions and acts".

In this regard, the APDCM has followed the line began in 2008 when the CUMPLE was implemented (Aid System for Controllers of Publicly-Owned Files to Fulfil their Obligations in Data Protection Matters) and DEPD (Telematic Exercise of Data Protection Rights).

Therefore, in 2009, it was decided to totally renew the APDCM's institutional portal by designing a virtual training program in collaboration with ICM, and finally to implement a tool for improving institutional relations by e-mail.

7.2. APDCM'S NEW INSTITUTIONAL PORTAL

The prime objective of the APDCM's new institutional portal is to give the individual citizen a clear idea of the APDCM's role in the defence of fundamental data protection rights in a more effective and user-friendly way. Another objective is to give better information, raise awareness and make it easier to exercise rights via the Internet.

We have also updated and modernised the graphic interface to make navigation easier and make it more intuitive and usable. To do this, some sections have been restructured to include audio and video download areas, including being able to view in *streaming* format, which was not possible before.

7. E-GOVERNMENT

So that each group can access the information required, seven intuitive clearly labelled channels have been set up with a list of contents. Specifically, there is the "The Agency", channel which provides institutional information about the Agency, its structure and how the organisations comprising it work, as well as the service letter, the APDCM's management indicators and the collaboration agreements signed by the Agency.

The "Citizens" channel sets out data protection principles as well as the rights that help individuals and the way to exercise them. As an essential supplement to this presentation, the portal also provides the opportunity to exercise these rights through the Internet using Madrid Regional Government digital signature mechanisms and remote registration. This same channel can also be used to submit queries to the APDCM and consult the File Register, and anyone who does not have a digital signature or prefers to contact the Administration using more traditional methods can download forms.

View of the "Citizens" channel.

The "Data Controllers" channel includes all the information required to be able to notify the personal data files to the APDCM and the forms needed for such, the models of third party service provision contracts, technical specifications for contracting external security audits and security documents for automated files and manuals. Access is also provided to the CUMPLE program developed by the APDCM to make it easier for file controllers to carry out their duties in the different areas, including file declaration through the Internet if they have digital certificates, safety audit management, security document preparation and attention to ARCO rights.

View of "File Controller's" channel.

In the "Events and Projects" and "Publications" channel, the activities of the APDCM in these fields are described and publicised. Updated information is given, including access to the presentations and audios from the training events conferences organised by the Agency, as well as free access to the Agency's digital publications *www.datospersonales.org* and *Data Protection Review*.

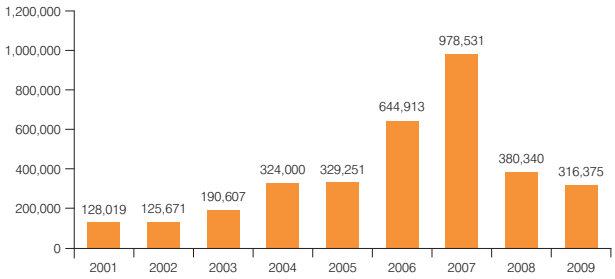
The "Legislation and Jurisprudence" channel contains the major international, national and regional regulations concerning data protection, with APDCM recommendations and instructions, as well as extracts from the most important sentences of different courts.

Finally, the "Consultations and Decisions" channel includes al the decisions issued by the APDCM on the infringement and data protection rights proceedings dealt with as well as a summary of the replies given by the Agency to the most frequent or interesting queries in each of the most important activity sectors under its supervision.

Regarding access to the APDCM's web page, in 2008 there was a total of 316,375 requests for access (data supplied by ICM). It should be emphasised that the drop in requests for access compared to 2008 was because the changeover to the new institutional portal meant that the old portal was not updated for three months.

The differences in access from 2007 to 2008 and in 2009, as we mentioned in the 2008 Report (see section 6.4 of the Report), are due to the change in the way of calculating the number of accesses, by counting connections and not individual access to pages.

APDCM Web Site Requests
Comparison of recent years



7.3. VIRTUAL TRAINING

This new virtual course arose from the Agency's wish to address the training needs of public employees, which led us to prepare a virtual tool, in collaboration with ICM that would facilitate even more personal data protection training.

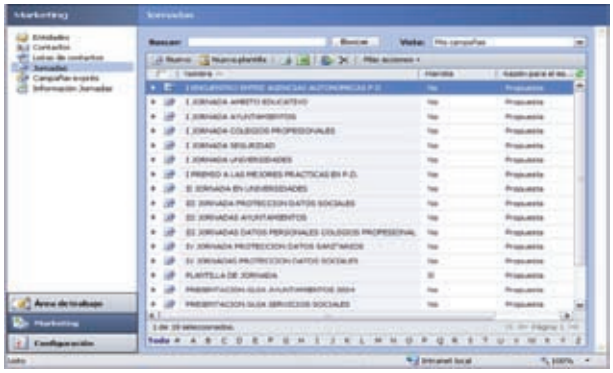
The Virtual Personal Data Protection Training Program consists of 15 teaching hours and is structured in two large blocks: the principles and rights of personal data protection and practical guidelines for controllers and public employees to meet their obligations.

The Program uses animations to introduce each of the chapters, is fully commented and proposes different kinds of practice and tests to help comprehension of the subject and check the knowledge acquired. The help of tutors is available to students throughout the course to encourage them and help answer questions and solve any problems that may arise. The course includes an in-class exam at the end so that students can obtain a certificate to show they have successfully passed the course.

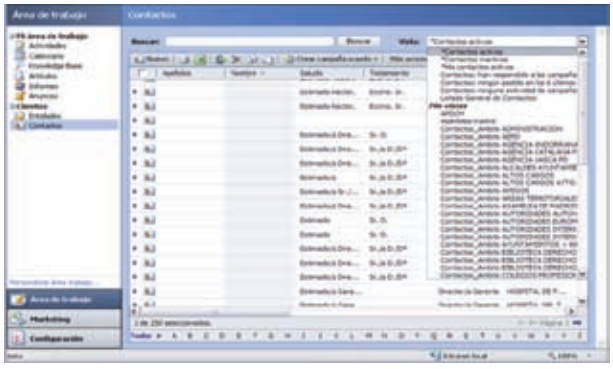
Finally, the APDCM received 1289 applications from Madrid Region public employees to do the *on-line* course.

7.4. CRM (CUSTOMER RELATIONSHIP MANAGEMENT)

This is a computer system whose main use is to improve the management of the APDCM's institutional relations. *CRM* enable a *data warehouse* to be administered with all the Agency's institutional contacts.



One of the main purposes of *CRM* is that the different calls for the conferences and acts organised by the APDCM can be more efficiently and effectively managed.



8. Training, Dissemination and Knowledge Management

8. Training, Dissemination and Knowledge Management

8. TRAINING, DISSEMINATION AND KNOWLEDGE MANAGEMENT

8.1. CONFERENCES AND TRAINING

Since the founding of the APDCM, one of its main objectives has been to make it easier for Madrid Regional Government Controllers to comply with Data Protection regulations by advising and training centre and public service staff.

Various methods have been used by the agency to achieve this objective: assigning consultants to the area of education in a way that is specific and suited to each data controller so that they can answer any queries raised by public managers; scheduling an exhaustive training programme at different levels; issuing specific publications for all levels of the area of education, which were distributed free of charge to all controllers and in training courses; and finally organising workshops to make known certain specific content of the Data Protection Regulations. Different heads of institutions from the Madrid Regional Government, Town Council, Professional Associations and the University were invited to take part in these conferences.

The implementation of the virtual training program would also need to be added to the acts referred to in the above paragraph. These were referred to in section 7.3 of this Report.

In this respect, the aim of the Conferences held in 2009 was to continue the line begun in 2008, that is, to publicise the main implications of the new Implementation Provisions of the LOPD throughout the different sectors. The new CUMPLE e-Government tools were also presented, aimed at making it easier for data controllers to comply with the LOPD, and DEPD, and aimed at enabling individuals to be able to exercise their ARCO rights (access, rectification, erasure and opposition) via telematics. In the area of security, a sector Handbook on the subject was also presented.

One of the sectors with most demand, the Education sector was also addressed. The 3rd Conference was held in 2008 and 2009 saw the 4th Conference. A conference was also organised dedicated exclusively to Secondary Education Counselling Departments.

As is now the tradition, each conference had a platform where data controllers could describe their experiences. These Workshops were held in institutional buildings linked to the public targeted.

These Conferences were as follows:

PROGRAMA

9:15 Entrega de documentación

9:30 Inauguración

9:45

10:15

10:45

11:15 Descanso

11:45

12:15

12:45

13:30 Coloquio

13:45 Clausura

Objetivos:

Dirigido a:

Lugar de celebración:

Inscripción:

PROGRAMA

9:15 Entrega de documentación

9:30 Inauguración

9:45

10:45

11:15 Descanso

12:15

12:45 Coloquio

13:00

14:00 Clausura

Objetivos

Dirigida a

Lugar de celebración

Inscripción

PROGRAMA

9:15 Entrega de documentación

9:30 Inauguración

10:00

10:45

11:15 Descanso

11:45

13:15

13:45 Coloquio

14:00 Clausura

Objetivos

Dirigida a

Lugar de celebración

Inscripción

9:30 Entrega de documentación

9:45 Inauguración

Sra. Dña. Teresa Cubello

10:00

10:45

11:45

12:15 La experiencia práctica en la orientación educativa

Sra. Dª. Carmen González Madrid

Sr. D. Juan Alfaro Moreno Cabrera

Sr. D. Julián Palacios Sánchez

13:15 Consultas frecuentes planteadas en el ámbito de

Sr. D. Francisco Javier Sempere Sanzorrigo

Coloquio

14:00 Clausura

Sr. D. José Manuel Arribas Alvarez

Objetivos

- Dar a conocer las implicaciones del nuevo Reglamento de Desarrollo de la LOPD
- Exponer la situación de los tratamientos de datos, así como los problemas surgidos en la aplicación de las medidas de seguridad
- Compartir experiencias reales de los tratamientos de datos en el ámbito educativo respecto a la implantación de la normativa. Difundir la experiencia de esta implantación y analizar las dificultades y soluciones adoptadas por parte de los centros de enseñanza.
- Difundir la normativa y los criterios de interpretación sobre protección de datos a los responsables de ficheros.

Dirigida a

- Directores de equipos de orientación y atención temprana en sus diferentes especialidades
- Orientadores
- Tutores
- Personas relacionadas en la información y orientación de menores y jóvenes de diferentes niveles

Lugar de celebración

Salón de actos del I.E.S. Virgen de la Paloma

C/ Ramón Rodríguez, 106

28039 MADRID

ATTENDEES	
4th Schools Conference	222
2nd Security Conference	160
2nd Local Police Conference	145
Guidance Team Conference	450

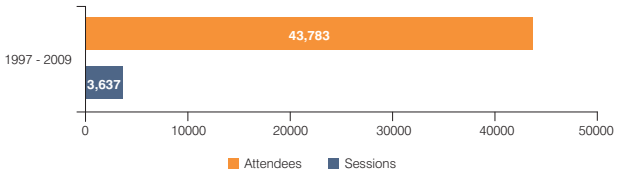
This training work is not only carried out through the Conferences mentioned above, but also by holding advisory sessions for public employees. These advisory sessions may have both a general and a specific content (for example, sessions aimed at members of a professional body or health workers).

INDICATOR	2007	2008	2009
Information sessions	316	305	199
Number attendees information sessions	3853	3880	3145

The drop in the number of information sessions and attendees is for two reasons: the first is the implementation of virtual teaching (see section 7.4 of this Report), which, as already mentioned, received 1289 applications to do this *on-line* course; the second is, as the APDCM has carried out very intense training work since its foundation, the demand for training from file controllers has stabilised or even declined in recent times.

During the 1997-2009 period the APDCM held a total of 3637 information sessions which were attended by 43,783 public employees.

Information Sessions and Attendees



Finally, we should underline that the APDCM gave a specific three-day conference, organised by the Madrid Regional Government's Directorate General of Consumer Affairs, to personnel from the State Government, Autonomous Regions and Local Corporations who provide their services in consumer departments.

8.2. APDCM Participation in Seminars

In 2009 the APDCM participated in numerous seminars, conferences and information sessions at a national and international level in which it was invited to inform of its experience as a guarantor of the fundamental right to personal data protection. Listed below are some of the most important events:

1. At a national level:
   - Master's in Telecommunications and Information Technology Law. "Foreigners and Data Protection". 21 January 2009. Carlos III University, Madrid.
   - Data Protection Dissemination Conference. 5 February 2009. Organised by the Bar Association.
   - Seminar on "Data Protection in Public Administrations". Paper: "Data Protection in the Madrid Region". 25 March 2009. Organised by Socinfo.
   - Social Cooperation Conference Guadalajara. Paper: "Social Networks and Privacy". 26 March 2009.
   - Melilla Technology Conference. Paper: "Data Protection in Public Administrations". 15, 16 and 17 April 2009. Organised by the President's Office and the Melilla Citizens' Participation Organisation.
   - 6th Health Data Protection Forum. 20 and 21 May 2009. Organised by the S. E. I. S.
   - New Challenges in Data Protection Issues. 1st Data Protection Conference: Enterprise and the LOPD. Cáceres, 21 May 2009. Conference organised by ADATEX (Entrepreneurs Association for Data Protection and Information Security in Extremadura).
   - Social Networks Conference. 16 June 2009. Madrid Bar Association.
   - Conference on Data Protection in Public Administrations. 28 and 29 June 2009. 29 June 2009. Organised by Dintel.
   - 2009 Telematics Security Course. Paper: "Data Protection Agencies in the Autonomous Regions". 2 July 2009. University of Vigo.
   - Public Presentation of the *Data Privacy Institute*. 14 July 2009. Closing Ceremony. Organised by ISMS Forum Spain. Assembly Room. General Council of Medical Associations in Spain.
   - Clinical History: confidentiality and access. Paper: "Data Protection and the Health Services. New Data Protection Regulations". 16 October 2009. Government of Castile and León, Health Department.
   - "Document Management as a Way of Complying with the LOPD". 27 October 2010. Round Table organised by Computerworld.
   - Master's in Basic Rights and Freedoms. Course: New Dimensions in Rights. Conference: "Personal Data Protection, Current Problems". 19 November 2009. Organised by the University of Castilla-La Mancha. Faculty of Legal and Social Sciences. Toledo.

– Data protection and information technologies in the health sector. 13th Madrid Region Rheumatology Society Congress. 10 December 2009.

– Course on the Mediation and Solving of Cyber Conflicts. Young People. Paper: "Data Protection in the Area of Education". 11 and 12 December 2009. Organised by IAITG and CEU.

2. At an international Level:

– Mexico National Transparency Week. Paper: "Personal Data Protection and Rectification as a National Policy". 27, 28 and 29 April 2009. Organised by the Institute for Transparency and Access to Public Information of the State of Mexico and Municipalities. State of Mexico.

– 6th International Seminar on Personal Data Protection –Successes and Innovations- towards the bicentenary of the Republic of Argentina. Paper: "Personal Data Protection at a Regional, National and International Level". 14 May 2009. Organised by the Personal Data Protection Agency of the Government of Buenos Aires (Argentina).

– Launch of the Personal Data Control and Regulatory Unit. Data Protection Conference. 15 May 2009. Legislative Palace Function Room. Montevideo (Uruguay).

– Congress on "Personal Data Privacy and Protection". 29 May 2009. Oporto (Portugal).

– Seminar on "Data Protection for Police and Judicial Cooperation in Criminal Matters: EU Requirements". 4 and 5 June 2009. Sarajevo (Bosnia-Herzegovina).

– Seminar on "The Fight against Cyber Crime". 28 and 29 September 2009. Tbilisi (Georgia).

– 5th Ibero-American Congress on Computer Security CIBSI'09. Conference: "Data Protection and the Design of Personal Data Processing". 16 to 18 November 2009. Montevideo (Uruguay).

– Seminar on "Data Protection for Police and Judicial Cooperation in Criminal Matters: EU Requirements". 10 and 11 December 2009. Bucharest (Rumania).

8.3. AWARDS

8.3.1. European Award for the Best Public Practices in Data Protection. Fifth Edition

This European Award, whose first edition was convened in 2004, was created by the APDCM to raise awareness of the fundamental right to data protection among data controllers working for European Public Administrations, as well as among public employees involved in any stage of personal data processing. The award is also in recognition of the most outstanding experiences or projects within the European framework, while also allowing them to be used by other European Public Administrations.

What the APDCM ultimately seeks with this award is to publicise the best data protection practices proposed or implemented by any authority or institution of the Public Administration of any country signed up to the Council of Europe Agreement of 28 January 1981 for the protection of individuals in respect of automated personal data processing.

Below are the award winners of the 5th edition.

5th EDITION AWARD WINNERS

Madrid Regional Government Department of Education. "Creation of an Academic History e-Register".	Alcobendas Town Council. "Alcobend@sprotect your data".	Association of Basque Municipalities (EUDEL). "Good Practice Handbook". Crossroads Bank for Social Security (Belgium. "Security".

The act to award the prizes of the 5th edition took place on the 18 February 2009 and was attended by many European and national authorities and personal data protection experts as well as the heads of the seventeen projects that had put forward their candidature.

The prizes were awarded by Mr Alfonso Cuenca Miranda, Deputy Minister for Justice and Public Administrations of the Madrid Regional Government.

Representatives from Alcobendas Town Council, winners of the 5th Edition of the European Award for the Best Public Practices in Data Protection with the "Alcobend@sprotects your data" project.

8.3.2. Award for the Best Scientific Paper on Data Protection

By convening this award, it is hoped that greater public awareness will be raised concerning "the data protection culture", basically through the transmission of the knowledge inherent in the dissemination of scientific, technical or legal papers linked to personal data protection.

In this way, the Madrid Regional Government Data Protection Agency seeks to promote research work, in the form of papers, which from a legal, scientific and economic, technical or social point of view, approach the theoretical and practical aspects deriving from processing the personal data of identified or identifiable natural persons.

As a result, the works submitted for this award must be unpublished, and be about personal data protection, either from a strictly theoretical standpoint or deal with the study and analysis of specific experiences that have had an impact on this subject, the analysis being conducted with all the scientific and academic rigor to be expected of this kind of award.

Although two candidates were nominated for this award, by means of the Decision of 23 October 2009, the Director of the APDCM, declared the award void.

8.4. TRAINING UNIVERSITY STUDENTS

Following the lines marked out by previous years, and by virtue of the Collaboration Agreements signed by the APDCM with different Public Universities in the Madrid Region, university student training has continued.

These practices deal with familiarity with data protection regulations, how the APDC Data Register works, how the APDCM Citizen's Advice section works, the legal analysis of inspection proceedings, rights protection and disciplinary proceedings, and the analysis of a data controller's duties. Students also examine case studies and produce legal reports.

CARLOS III UNIVERSITY	
Academic Training DEGREE IN JOINT STUDIES (LAW)	
PERIOD	STUDENTS
March/May 2009	4
July 2009	4
AUTÓNOMA UNIVERSITY	
Academic Training DEGREE IN LAW	
PERIOD	STUDENTS
April/May 2009	4

8.5. "PABLO LUCAS MURILLO DE LA CUEVA" RESEARCH AND DOCUMENTATION CENTRE

By means of the Decision of 28 January 2008, the Director of the Madrid Regional Government Data Protection Agency proceeded to establish and put into service the "Pablo Lucas Murillo de la Cueva Research and Documentation Centre", part of the Madrid Regional Government's Data Protection Agency.

Setting up this Centre has promoted research work, which, from a legal, scientific and economic, technical or social point of view, tackles the theoretical and practical aspects deriving from processing the personal data of identified or identifiable natural persons. It also opens up a new way of making people aware of the fundamental right to personal data protection by creating a specialised space to serve as a point of reference to provide a service not only for Regional Government, but also for other national and international authorities and for interested students or individuals requiring information on such an important right as personal data protection.

In 2009, the documentary collection of this Centre was extended by 204 publications and currently has a collection of over 2000 publications and 20 specialist reviews.

On 24 June 2009, Mr Miguel Ángel Davara donated 124 books from his private collection to the "Pablo Lucas Murillo de la Cueva" Research and Documentation Centre.

In addition, a link has been established through the APDCM's web page so that inquiries can be dealt with concerning its bibliography.

9. Publications

9. Publications

9. PUBLICATIONS

9.1. SECURITY AND PERSONAL DATA PROTECTION

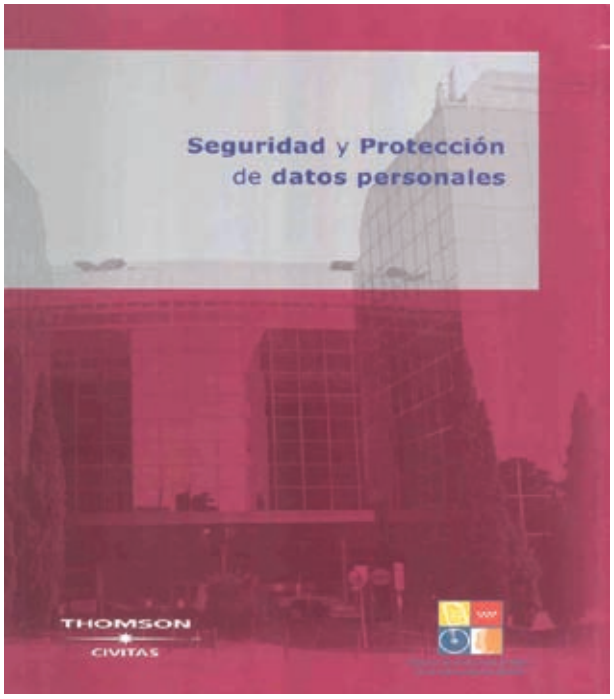
In 2009 the APDCM prepared and published the sector handbook on "Security and Personal Data Protection". The handbook is intended for data controllers and security heads who need to know the security measures that can be applied to the system administrators of the protected files, and above all personal data users.

Security measures are analysed for automated and manual files as set forth in Royal Decree 1720/2007, of 21 December, governing the Implementation Provisions of Organic Law 15/1999, of 13 December on personal data protection, in order to facilitate implementation and compliance by analysing the risks and threats of the current state of technology and recommending some rules of behaviour for the personnel that handle protected data.

Since the Regulations are legislative they only specify the requirement to meet certain measures without explaining the fundamentals or dangers that make these measures essential. This is because, due to their very nature, the laws or legislative regulations do not usually go into the causes giving rise to such regulations, but only make a superficial reference to them by enumerating the mandatory obligations or measures.

It is fundamental for personal data users and administrators to be warned of the dangers and threats and what each of them can do to defend the security of data that is their responsibility. One of the aims of this publication, therefore, is: to explain the techniques that are currently used to attack data security and explain the *best practices* for defending oneself from these attacks, in a way that can be understood by the average user.

With this publication we follow the line begun in 2008 with the publication of sector handbooks on *Personal Data Protection for Public Health Services, Personal Data Protection for Local Authorities, Data Protection for Public Universities, Personal Data Protection for Public Social Services, Personal Data Protection in Public Corporations, and Personal Data Protection in State Educational Institutions* and these are now complemented by the publication of the *Personal Data Protection Handbook for Public Employees.*



9.2. REVIEWS

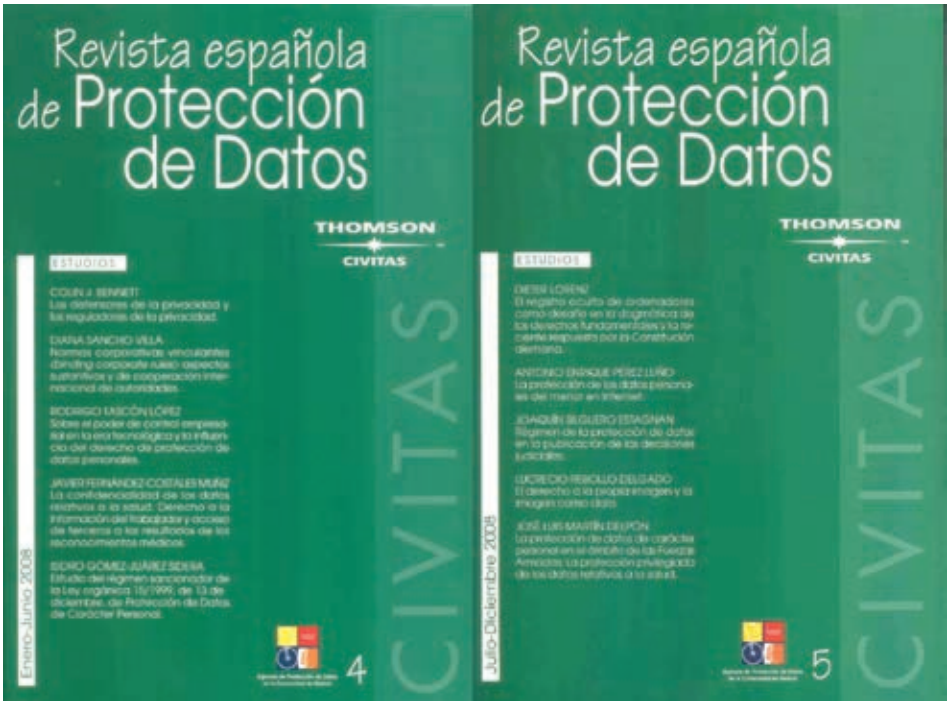
9.2.1. Spanish Data Protection Review

In 2007 the *Spanish Data Protection Review (SDPR)*, directed by the APDCM and published by Thomson-Civitas first appeared. Its aim was to provide a platform for doctrinal papers on the fundamental right to data protection, and which were well-developed from a scientific point of view.

The *Spanish Data Protection Review* is a mainly *legal* journal which studies personal data protection legislation and passes judgement on the actions of public powers and individuals. Notwithstanding, personal data protection is a field where clearly defined interests and values come into conflict, and the problem is to protect the freedom of automated systems while at the same time allowing public administrations and enterprise do their work. For this reason, the Review does not confine itself to a *lege lata* analysis but also aims to address the demands of society in this respect by contributing *lege ferenda* proposals and offers the courts criteria for interpreting legislation that takes account of the effectiveness of various solutions. This Review has a vocation not only for contributing material that publicises legislation but which also diagnoses problems and puts forward solutions as part of its commitment to a more just society. Therefore, this Review publishes any reflections on *political science*, which rigorously and without demagogy, attempt to justify what values should be given priority in the different scenarios. This helps people who defend one particular opinion on personal data protection and those who have different convictions, to reflect, thereby contributing in some way to understanding –to internalising- the various interests at stake.

The Review, which comes out every six months, has sections on “Studies”, “Comments on Legislation and Case Law”, “Book Reviews”, “Documents” and “The Forum”. An Editorial Committee has been set up comprising professors from various areas of research –Administrative Law, Criminal Law, Labour Law, Civil Law, International Law, Constitutional Law, and Health Legislation- who work systematically to evaluate the content.

2009 saw the publication of numbers 4 and 5 of the *Spanish Data Protection Review*.



In order to find out whether or not the *Spanish Data Protection Review* can be considered to be a publication with scientific impact, it was subjected to a rigorous study by one of the members of the review's Assessment Committee. The outcomes of this study can be seen in the changes introduced, beginning with the fourth edition of the review. Once these changes had been made we requested it be included in international and specialised data bases, for which it was submitted to an evaluation procedure by the Centre for Human and Social Sciences of the Higher Council for Scientific Research, whose work is focused on selecting publications for the ISOC data base that cross a specific threshold of publishing quality and scientific-technical interest.

The evaluation was positive with the *Spanish Data Protection Review* being considered to be of scientific impact. It was therefore admitted and included in the C-Normal category.

9.2.2. Digital Review www.datospersonales.org

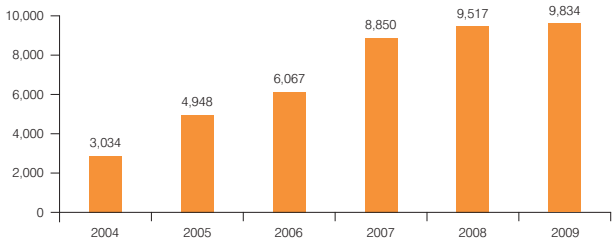
Founded in 2003, the digital review *www.datospersonales.org* has become a point of reference among publications that deal with the different aspects of the fundamental right to personal data protection right down to the last detail.

This digital review, which comes out every two months, has currently published 42 numbers, 6 of which were published in 2008.

The papers published by experts in 2009 examined, among other things, such wide-ranging issues as the invisible dangers of privacy on the Internet, foreigners and data protection, SITEL, research into medical health and the right to privacy, present and future security measures and the compliance officer in relation to personal data protection.

The other content of the review has also been made more substantial (national and international news, case law and publications), with emphasis being placed on the channel referring to international legislation, where experts on the matter analysed Sentence 155/2009/2009 of the Constitutional Court of 18 May 2009 rejecting the appeal for legal protection number 1682/2007, basing the decision on the alleged violation of the fundamental right to use the relevant evidence for its defence and the fundamental right to communicate or receive truthful information by any means of dissemination, and the Sentence 159/2009 of the Constitutional Court of 29 June, appeal for legal protection 9914-2006, on the transfer of health data within the framework of a selection procedure.

Nº. subscriptions **Annual evolution of subscriptions**



9.2.3. Digital Review www.dataprotectionreview.eu

The Madrid Regional Government Data Protection Agency started to publish the digital version of the Data Protection Review in English in October 2006 (*www.dataprotectionreview.eu*), and in 2009 published three new numbers.

The purpose of *www.dataprotectionreview.eu* is to bring the data protection culture to all those who have a professional interest in the legal and technical aspects of data protection and whose first or second language is English. The review is therefore aimed at a wide international audience made up of the members and employees of data protection authorities, university teachers, students, professionals, civil servants, lawyers, non-governmental organisations and any individuals interested in having updated information on privacy and data protection.

To this end, www.dataprotectionreview.eu is structured into four channels:

1. *Commissioner's Corner*: Reserved for the commissioners, presidents or directors of data protection control authorities so they can express their opinions on matters of concern or issues on which their authorities have done some special work. In the numbers published in 2009 on this channel, we were able to read the following papers:
   - The Guantanamisation of Data. Natasa Pirc Musa. Information Commissioner of the Republic of Slovenia.
   - Would the personal data be protected when court decisions are published and made available? Marijana Marusic. Director (Directorate for Personal Data Protection of Macedonia).
   - The Federal Institute of Access to Public Information as the Guarantor Entity for the Protection of Personal Data. Jacqueline Peschard. Representative President of the Federal Institute for Access to Public Information of Mexico (IFAI).

2. *Experts' opinion*: as the title indicates, this contains papers by experts in the subject. Some of those who made contributions are:
   - Communications and External Relations Strategy in the Information Commissioner's Office (ICO). Susan Fox. Director of Communications and External Relations Information Commissioner's Office (United Kingdom).
   - Organizational Motives for Adopting Privacy Enhancing Technologies (PETs). John Borking. Former data protection commissioner of The Netherlands. Owner/director of Borking Consultancy in Wassenaar (The Netherlands).
   - Recent Developments in Israeli Data Protection Law: En Route to European Standards. Omer Tene. Associate Professor, College of Management School of Law and legal consultant.
   - Open Space Privacy Dialogue at PrivacyOS Conferences. Katalin Storf. PrivacyOS Project Coordinator. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD).
   - Data protection auditing, problematic and challenges. Dina Kampouraki. Leading auditor in the Greek Data Protection Authority.
   - Are Users of Social Networking Sites Subject To Data Protection Law, As Controllers? Douwe Korff. Professor of International Law. London Metropolitan University. London (UK).
   - What Outcomes Should Regulation Achieve for Individuals, Regulators and Society? Charles Raab. Professor Emeritus and Honorary Professorial Fellow, School of Social and Political Science, University of Edinburgh.
   - Social Networking Sites and Freedom of Expression. Douwe Korff. Professor of International Law. London Metropolitan University. London (UK).

3. *In the last four months*: This section aims to provide readers with a summary of the most important and interesting events that have happened in the world in connection with privacy and data protection.

4. *Regulation and Case Law*: References, reviews and comments on new acts and regulations as well as case law, on every level: regional, national, European or international.

5. *Decisions and Opinions*: This section contains the decisions, opinions, guidelines, instructions or recommendations produced by any data protection authority in the world that may be of general interest for the international data protection community.

9.3. MONOGRAPHS ON DATA PROTECTION

Following the line begun in 2003 to take part in and promote initiatives of unquestionable didactic and doctrinal interest that make a doctrinal contribution to the understanding and analysis of problems arising out of the fundamental right to personal data protection, the Agency co-published a new monograph in 2009 with Aranzadi-Civitas Publishers, as part of their "Data Protection" collection.

9.4. SECTOR INFORMATION LEAFLETS ON DATA PROTECTION

These leaflets are intended for individuals who use the public services provided by the different Public Administrations in the hope that they will make them more aware of their fundamental right to personal data protection.

For this reason the leaflets have been written in plain simple language so that all individuals will be able to understand their rights in this matter.

Moreover, since the leaflets have been prepared for health centre and social services centre users, the content of the leaflets has been adapted to the specific circumstances of each sector.

Therefore, 35,000 copies of the personal data protection leaflet for public health services and 15,000 copies of the personal data protection leaflet for social services were distributed throughout the different health service and social service centres.

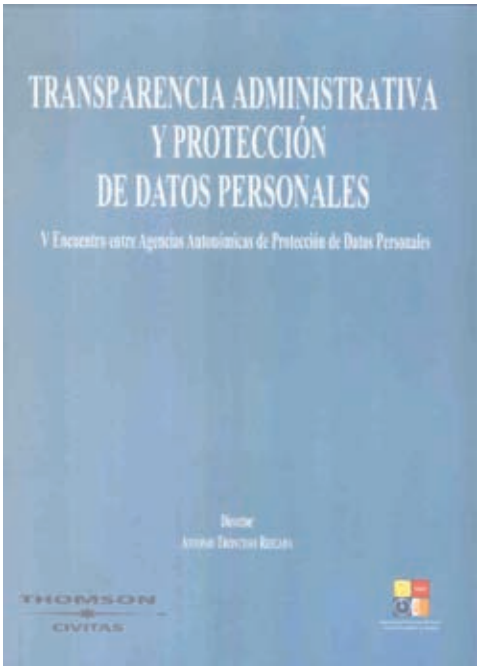
9.5. ADMINISTRATIVE TRANSPARENCY AND PERSONAL DATA PROTECTION

This book contains the papers presented at the 5th Meeting of Regional Government Data Protection Agencies held in Madrid on 28 October 2008. That conference was an opportunity to analyse what criteria should be adopted to reach the right balance between administrative transparency and the fundamental right to data protection.

This book approaches the question from a doctrinal standpoint with the participation of different academics, and examines the said question from a comparative perspective with contributions from different Control Authorities that are responsible for personal data protection and guarantee access to public information. The book also has the participation and opinions of the spokespersons of the parliamentary groups on the Chamber of Deputies Public Administration Committee as well as the opinions of representatives of civil society.

Since the 5th Meeting of Regional Government Data Protection Agencies was a good opportunity to examine the Implementation Provisions of the LOPD, the book contains the papers presented by the public employees of the four Data Protection Agencies in Spain, within the framework of the meeting.

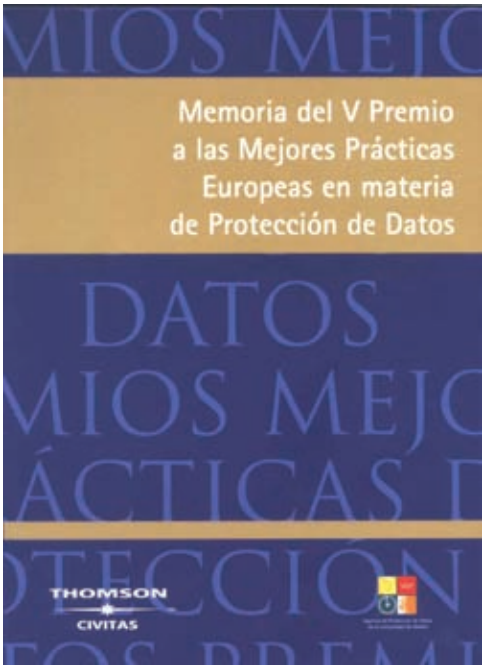
The book, *Administrative Transparency and Personal Data Protection* was presented at the headquarters of the APDCM on 17 September 2009 at an act presided over by the Deputy Minister of Justice and Public Administrations for the Madrid Regional Government and was also participated by the Director of the APDCM, the Directors of the Spanish Data Protection Agency, the Catalonian Data Protection Agency and the Basque Data Protection Agency.



9.6. Report of the 5th Edition of European Award for the Best Public Practices in Data Protection

It not only contains the work of the candidates put forward at the 5th Edition of the Award, which were seventeen in all, but also the work of the candidates put forward at the four previous editions of this award.

Since the purpose of the award is not only to recognise the work done by the different Public Administrations that have incorporated personal data protection into their procedures, but also the transfer of knowledge through the 5th Edition Report. The file controllers can use the different work of the candidates put forward to adapt their respective procedures to personal data protection. In other words, apply knowledge management.



10. Citizens Advice Service

10. Citizens Advice Service

10. CITIZENS ADVICE SERVICE

The Citizens Advice Service of the Madrid Regional Government Data Protection Agency is to be found in the Specialised Information Offices that comprise the Regional Government's horizontal Information System. This service's priority is to provide individuals with information and guidance on rights that are recognised in the personal data legislation currently in force and to contribute to publicising this fundamental right.

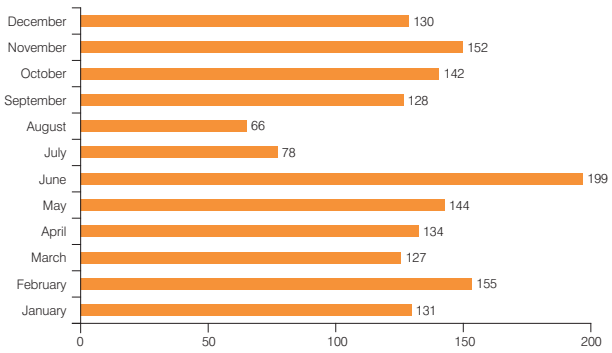
The Citizens Advice Service reports to the General Secretariat's Office in accordance with the rules set forth in article 20 of Decree 40/2004, of 18 March governing the Agency Statute.

The Citizens Advice Service, as stated in previous Reports, is the first point of contact for any individual who wishes to obtain information on the principles and rights relating to individuals as set forth in Organic Law 15/1999, of 13 December on Personal Data Protection (hereon, the LOPD), in Act 8/2001, of 13 July on the Protection of Personal Data of the Madrid Regional Government, and on other legislation applicable to this matter.

In order to comply with the obligations described above, the Citizens Advice Service of the Madrid Regional Government Data Protection Agency places various channels at the citizen's disposal:

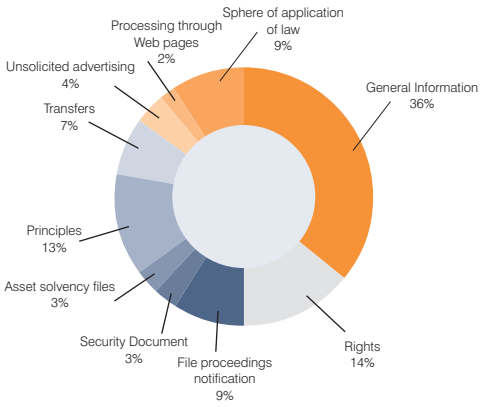
- By email *apdcm@madrid.org*.
- Through the digital review, *www.datospersonales.org*.
- By telephone on 91 580 28 74/75.
- By fax on 91 580 28 76.
- Face-to-face attention and by ordinary mail at the headquarters of the Madrid Regional Government Data Protection Agency whose address is Calle Cardenal Marcelo Spínola, No. 14 (28016-Madrid).

The total number of queries attended in 2009 was 1586.

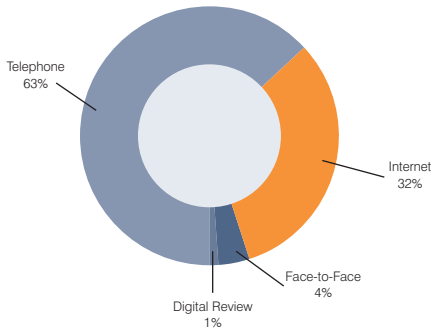


10. CITIZENS ADVICE SERVICE

Graph 1. Analysis by Subject



Graph 2. Analysis by Media



Of all the queries, the most relevant are:

- The information required to be provided on the forms used by the Madrid Regional Government to collect personal data.
- If personal data published in the *Madrid Regional Government Official Journal* could possibly be picked up by a search engine and be at the disposal of anybody.
- A pharmacy requesting that a health centre should provide them with information about a patient so as to be able to contact them to inform of a mistake in the medicine supplied.
- Application of the LOPD to the representatives of legal entities.
- When a hospital denies access to a clinical history, what is the correct procedure to follow.
- A patient's request to a doctor to anonymise their personal data.
- An institution's publication on its website that the agreements of its governing collegiate body should include the name and surname of the interested party.
- Application of the LOPD to hard copy administrative files.
- The possibility to view the images of a video tape, through which, allegedly, the author could be accused of abduction.
- The legality of a survey asking about health data, including the data of members of the family, in order to participate in a university competition.

11. Collaboration between the APDCM and other Control Authorities and Institutions

11. Collaboration between the APDCM and other Control Authorities and Institutions

11. COLLABORATION BETWEEN THE APDCM AND OTHER CONTROL AUTHORITIES AND INSTITUTIONS

11.1. INTER-AGENCY WORKING GROUPS

Within the framework of the principle of institutional loyalty that predominates in the relations between the different Data Protection Agencies in Spain (Spanish Data Protection Agency, Catalonian Data Protection Agency, Basque Data Protection Agency and the Madrid Regional Government Data Protection Agency), various working groups have been set up to bring together the different views on interpretation and open up a debate on any topical questions. The working groups currently existing in this context are as follows:

- Directors.
- Register, coordinated by the Spanish Data Protection Agency.
- Inspection, coordinated by the Madrid Regional Government Data Protection Agency.
- Legal and regulatory analysis, coordinated by the Catalonian Data Protection Agency.
- Organization, Modernisation, Communication and Training, coordinated by the Basque Data Protection Agency.

11.1.1. Directors Working Group

The Directors of Data Protection Agencies meet to mark out the strategic lines for collaboration between control authorities, monitoring them and finalising the decision-making process on matters that have been discussed in the different groups and which require the approval of the director's office for them to be implemented and set into motion.

In 2009, Agency Directors met at the APDCM Headquarters on 17 September, where each Agency Director reported on the meetings held with other groups that year.

Among other things, they also dealt with matters arising from the 31st International Conference organised by the AEPD, the adoption of International Privacy Standards, the current series of problems regarding the publication of personal data in official journals and gazettes and the innovations introduced in the File Registers of the respective Agencies by the Implementation Provision of the LOPD.

11.1.2. File Register Working Group

The File Register Working Group held two meetings in 2009, both by video conference.

The following are some of the questions dealt with by the Group:

- Review of the schemes to exchange information between Registers.
- The new RENO system: Inter-Register file exchange through *Web Services*.
- Document Functional Analysis "Register Information Exchange between RGPD and Regional Government Agencies".

11.1.3. Inspection Working Group

In 2008, this Working Group met on four occasions. Two of the meetings were held face-to-face at the Madrid Regional Government Data Protection Agency and another was held at the Catalonian Data Protection Agency headquarters. The other two meetings were held jointly with the Legal and Regulatory Working Group, one of the meetings being by video conference and the other face-to-face. The groups held a joint meeting as issues affecting both were dealt with.

The APDCM, as coordinator of this Working Group, takes charge of organising the Agenda as well as writing the Minutes of the meetings.

Among other matters, the Group dealt with the following questions:

- Rights protection procedures and the system for allocating responsibilities regarding the automatic indexing of the information published in official journals and gazettes that is performed by Internet search engines.
- The identification of postal workers by their Identity Card Number on acknowledgement of receipt forms.
- The nature of the files of the Compensation Boards.
- If it is possible to process a rights proceeding and a pre-information/disciplinary procedure at the same time when the affected party simultaneously lodges a formal complaint and a data protection demand regarding the same proceedings.
- Clinical/company responsibility for clinical documents.
- The nature of the files of Professional Associations on "monitoring collegiate action regarding deposits" and "monitoring action by the Associations regarding tenders".
- Registration of hospital clinical research files.
- The nature of the data files used by a municipal sports centre when managing the service by using a private password.
- If there is a possible conflict between the freedom of access to information and/or the principle of transparency and the duty of secrecy regarding the information appearing in Public Administration information publications.
- Analysis of the accumulation of proceedings (article 73 of Act 30/1992) and personal data protection.
- The possibility of Agencies being able to protect the exercise of the rights of rectification and erasure regarding data contained in the clinical histories of deceased persons, when this protection is requested by members of the family.

- Agency notifications using a courier company.
- Submission of notifications to interested parties via telematics in the event of the receivers of such notifications not meeting the requirements set out in articles 13 to 16 of Act 11/2007, of 22 June, regarding the e-Access of Individuals to Public Services.

11.1.4. Legal Analysis and Regulatory Working Group

In 2009 this group met on four occasions: two by video conference and the other two, as we have already stated, were joint meetings with the Inspection Working Group.

Among other matters, the Group dealt with the following questions:

- Application of article 2.3 of the Implementation Provision of the LOPD to Chamber of Commerce files containing data on their electors. Possible erasure of "Company electoral role", "Public company census" and "permanent Chamber of Commerce appeals" files.
- Scope of article 20.1, last paragraph of the Implementation Provision of the LOPD.
- Whether or not official journals should be classified as a file.
- Concept of an identifiable person (AVPD).
- Revelation of Identity Card Number when e-Documents are signed by Public Administration civil servants and authorities.
- Scope of article 35.3 of Act 11/2007, of 22 June, regarding the e-Access of Individuals to Public Services in respect of articles 6.2.b) and 9 of that Act.
- The role of credit card entities that collaborate with the Administrations to collect taxes. Collection procedure and the responsibility of the Administrations.
- The installation of video surveillance cameras in municipal facilities by an unauthorised security firm.
- The determination of the holders of the right of access to the clinical histories of deceased persons.

11.2. AGREEMENTS AND COLLABORATIVE ACTS

11.2.1. Signed Agreements

Following the traditional lines of institutional collaboration of the APDCM, whose objective is to establish appropriate ways to collaborate with other institutions in order to promote the development of joint programmes for a greater dissemination of the fundamental right to personal data protection, the APDCM has signed the following instruments of cooperation:

- Collaboration agreement between the Institute for Access to Public Information of the Federal District and the Madrid Regional Government Data Protection Agency.
- Collaboration Agreement between the Institute for Access to Public Information of the State of Oaxaca and the Madrid Regional Government Data Protection Agency.
- Collaboration agreement between the Institute for Transparency and Access to Public Information of the State of Mexico and municipalities and the Madrid Regional Government Data Protection Agency.

- Framework Collaboration Agreement between the Dintel Foundation and the Madrid Regional Government Data Protection Agency.

In addition, in conformity with one of the clauses established in one of the aforementioned agreements, the APDCM will take responsibility for the "data protection" of the *DINTEL Top Management–a+)) audit and security* review.

Finally, work was begun to sign the corresponding Collaboration Agreements with the Spanish Association of Privacy Professionals, the Committee for Data Protection in Andalusia of the Andalusian e-Commerce Association and the Data Privacy Institute.

11.2.2. Meetings with other Control Authorities

On 6 of November 2009, taking advantage of the 31st International Data Protection Conference, the APDCM held a reception at its headquarters for members of the Ibero-American Data Protection Network.

Using the occasion, the APDCM presented its main activities to the members of this network offering them the chance to purchase the Agency's publications.

Collaboration Agreements were also signed with the Ibero-American Institutions referred to in the preceding section of this Report.

11.3. CONFERENCES GIVEN BY THE DIRECTOR IN MEXICO, ARGENTINA AND URUGUAY

The Director of the APDCM gave various Conferences in Mexico, Argentina and Uruguay during a working trip in May 2009.

In the course of his trip to Mexico he had the opportunity to meet different Information Access Institutions, as well as attending a plenary session to examine the working methods regarding complaints made about the access to public documents and personal data protection.

At the invitation of the Argentinean Data Protection Authority, he took part in the Sixth National and International Seminar on "Personal Data Protection: Successes and Innovations on approaching the Bicentenary of the Republic of Argentina" with a conference on "Personal data protection at a national and international level: new and better practices".

The final stage of his trip took him to Uruguay, where he took part in the 6th International Seminar on Personal Data Protection -"Public and Private Information. Protection and Penal Issues", where he spoke about the Legal Framework of Public Data Bases. He also took part in the acts to celebrate the founding and commissioning of the Personal Data Control and Regulatory Unit, the new data protection authority established in the recent Uruguayan data protection act.

12. International Activity

12. International Activity

12. INTERNATIONAL ACTIVITY

12.1. 31ST INTERNATIONAL DATA PROTECTION CONFERENCE

The APDCM participated in the parallel session - "Sub-national, sub-state federated data protection authorities and Public Administrations: proactive strategies in education and health".

The session, chaired by the Data Protection Commissioner of the State of Berlin, was also participated by the Basque Data Protection Agency, the Catalonian Data Protection Agency, the Privacy Commissioner for Quebec, the Office of the Victoria Privacy Commissioner (Australia), the Office of the Ontario Privacy Commissioner and the Citizen's Commissioner of the Institute for Public Access to information of the Federal District of Mexico.

The APDCM Director referred to his speech on the actions undertaken in recent times by this Agency, highlighting the different actions taken to "publicise" the data protection culture. Among these actions he cited the new publications, *Personal Data Protection for Public Health Services, Personal Data Protection for Social Services, Personal Data Protection for Education, Personal Data Protection for Public Universities, Personal Data Protection in Public Corporations, Personal Data Protection for Local Authorities, Security and Personal Data Protection, the Personal Data Protection Handbook for Public Employees* and the digital reviews *www.datospersonales.org* and *www.dataprotectionreview.eu* and the scientific publication *Spanish Data Protection Review*.

During the Conference, the APDCM also had a stand to give information on these activities and hand out documents and publications to those attending.

12.2. EUROPRISE

The European Privacy Seal certifies that a product or service complies with European data protection and privacy legislation, which provides added value to the product or service in addition to a guarantee for consumers.

The EuroPriSe Privacy Seal *(www.european-privacy-seal.eu)* is issued by an independent product and ICT services certification authority after having successfully passed a two-stage assessment and verification procedure: an assessment by accredited technical and legal experts is verified by an independent, impartial certification authority, the Schleswig-Holstein Data Protection Authority (Unabhaengiges Landeszentrum fuer Datenschutz or ULD). The Seal as well as the public reports, offer transparent guidance when choosing or evaluating a product or ICT service from a data protection standpoint.

Within the framework of the EuroPriSe Seminar organised by the APDCM, held on 3 November 2009 in Madrid and specifically focused on dealing with topics related to the work of the data protection authorities, two new European Privacy Seal seals were awarded. They were presented by the Director General of European Affairs and Cooperation with the State, Mr

Antonio González Terol and Ms Kirsten Bock, Project Manager of the EuroPriSe Seal.

The seal was awarded to the Honourable Bar Association of Madrid (ICAM) for its "Free Justice Service Management Solution" and to the Spanish firm Iberemec S. A. for its "Iberemec CRM" customer relations management system. These two ICT services satisfactorily demonstrated their compliance with the demanding requirements of European data protection legislation.

Presentation of the Seal to the Honourable Bar Association of Madrid and EuroPriSe (ICAM) for its "Free Justice Service Management Solution".

Presentation of the Seal to Iberemec S. A. por for its "Iberemec CRM" customer relations management system.

12.3. PRIVACY OPEN SPACE (PRIVACYOS)

PrivacyOS is a European project headed by Unabhängiges Landeszentrum für Datenschutz (Schleswig-Holstein Data Protection Authority) in which the APDCM also takes part. It aims to set up a thematic network on the creation of privacy protection infrastructures. Coordinating this network would be done by holding a series of conferences that would follow the *"Open Space"* model. *Open Space* is a methodology developed in 1985 and widely used by NGOs, and international businesses and organisations. Its main function is to enable the agendas to be decided and changed while the meeting is being held. The ultimate purpose is to set up a long-term collaboration via a telematics network and set into motion connections with other European projects.

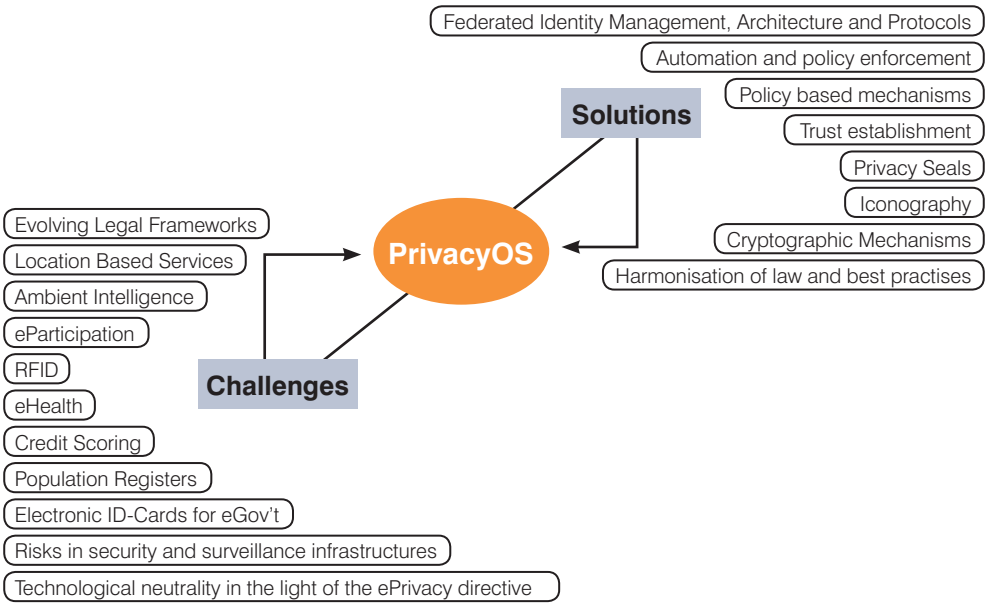
The First and Second PrivacyOS Confernces were held in 2009. At the first conference, held in Berlin on the 1, 2, and 3 of April, the APDCM presented the results of the Data Protection Information Plan for School Children (see section 6 of this Report).

This Second Conference, attended by representatives from ten countries, dealt with current issues, presented pilot projects and analysed the results of now acclaimed projects. Some of the topics discussed were: "the value of privacy in the Web", "definition and redefinition of PET", "the use of social networks among the young", "control of selective access to social networks", "the rapid response network", "iconography at the service of privacy", "e-Payment of road tolls: privacy" or "Web 2.0 encryption".

Regarding the Third Conference held in Vienna on the 26 and 27 October, the APDCM chaired the table on "Data Protection Authority Control Strategies", in which the Data Protection Authority of Slovenia took part.

At the same table, one of the APDCM representatives gave a conference on the action taken by the APDCM to create a data protection culture, insisting not only on publications but also on the work to support data controllers, underlining the recent launch of the CUMPLE computer application.

The conference also discussed issues such as spam and cyber crime and presented projects like Encore (dealing with the proceedings for giving and withdrawing consent), TOR (software project to help defend against web traffic analysis, a form of web surveillance that threatens personal freedom) and EuroPriSe.



12.4. PRIMELIFE

The APDCM was invited to take part in this Reference Group due to its intensive work on many European projects and its experience in promoting, raising awareness and supervising personal data protection to ensure that this fundamental right is duly taken into account in the project.

PrimeLife is a project that follows in the footsteps of the Prime Project (see section 11.3 of the 2008 Report). It will attempt to solve how to protect privacy in emerging Internet applications and how to ensure that such protection is maintained throughout our lives.

The Reference Group is made up of experts from different fields and undertakes a consultancy role to provide an objective, independent external vision for project members to enable them to evaluate their progress and outcomes so that society will be able to get the maximum benefit from the products and services that emerge as a result.

12.5. INTERNATIONAL CONTROL AUTHORITY CONFERENCES AND WORKING GROUPS

12.5.1. Data Protection Authorities Spring Conference

At this Conference held in Edinburgh in April 2009, the APDCM Director gave a speech on the results of the Data Protection Information Plan for School Children (see section 6 of this Report).

Also presented at the Conference were the two major points of the report, “Review of the Data Protection Directive” commissioned by the British Data Protection Authority *(Information Commissioner)* to the winner of the competition convoked to that effect.

This report gave way to a live debate among those attending, on its conclusions, and, in particular, on whether or not it is necessary to approach or initiate the procedure to modify the current legal framework of data protection in the European Union.

Likewise, the international context of regulation in matters of privacy was also approached, and, specifically, Mr Artemi Rallo, Director of the Spanish Data Protection Agency explained the state of the work that the AEPD is heading, with a view to setting an international standard in the subject of data protection to facilitate information exchange in a globalised world.

The Conference finally approved both documents on leadership on data protection issues in Europe and on the need to set common standards regarding international transfers to third party countries within the sphere of police and judicial cooperation, as well as holding next year’s Conference in Prague (Czech Republic).

12.5.2. Working Group for European Union Complaints

The APDCM participated in the two meetings of this group that took place in Prague on the 12 and 13 March 2009, organised by the Czech Republic data Protection Authority, and in Cyprus on the 22 and 23 October in Limassol, organised by the Cypriot Data Protection Authority. At the first meeting, the PADCM presented Instruction 1/2007 at a round table on video surveillance on personal data processing through camera or video camera systems in the sphere of bodies and Public Administrations of the Madrid Region. At the second meeting the outcomes of the Data Protection Information Plan for School Children were presented (see section 6 of this Report).

12.5.3. Telecommunications Working Group

The 45th Berlin Group Meeting was held in Sofia on the 12 and 13 March, which was attended by representatives from the APDCM.

The main items on the Agenda of the 45th Meeting were as follows:

- Personal data processing to pursue the violation of author's rights in p2p networks.
- Privacy and junk mail/e-recycling.
- Deep inspection technologies of packets and privacy.
- Proposal for a digital data protection and freedom of information charter.
- To obtain the resources needed for a cyber defence strategy in the sphere of data protection in telecommunications.
- The "private web-conscious life".
- CCTV in buses and taxis.
- Questions of privacy in social networks.
- Privacy impact assessment: case studies.

The outcome of the meeting was to adopt two final documents:

- A report on recommendations on data processing on toll roads (Sofia memorandum).
- A report on recommendations on data processing on junk mail.

12.5.4. 8th Ibero-American Conference

The APDCM was invited for the first time to take part in the Ibero-American Meeting. It took place in Madrid, organised by the Spanish Data Protection Data Agency in advance of the 31st International Conference.

Different papers on the applicable personal data protection legislation in Ibero-America were presented at the 8th Meeting.

13. General Secretariat

13. General Secretariat

13. GENERAL SECRETARIAT

The management of personal, financial and materials resources is undertaken by the General Secretariat of the APDCM. Together with these duties, we can also underline the following:

1. To hold the Secretariat of the Data Protection Committee. In 2008 the membership of the Council was renewed since the term of appointment established in article 17.3 of Act 8/2001 had expired (Decree 28/2008 of 18 December, *BOCM* of 23 January 2009), having held the founding session on 3 March 2009. At present, the Council comprises the following members:

   a) The Madrid Assembly: a representative from each parliamentary group.

      – The Honourable Mr Álvaro González López, for the Popular Parliamentary Group.

      – The Honourable Ms Rosa Alcalá Chacón, for the Socialist Parliamentary Group.

      – The Honourable Mr Luís Otero Fernández, for the United Left Parliamentary Group.

   b) The Madrid Regional Government: five representatives assigned by the President.

      – The Honourable Mr Alfonso Cuenca Miranda, Deputy Minister of Justice and Public Administrations of the Office of the Presidency, Justice and Interior.

      – The Honourable Mr Borja Sarasola Jáudenes, Technical General Secretary of the Office of the Vice-Presidency and the Government Spokesperson.

      – The Honourable Mrs Zaida María Sampedro Préstamo, Director General of Health Information Systems of the Department of Health.

      – The Honourable Mr Eugenio López Álvarez, Director General of Legal Services of the Office of the Vice-President and the Government Spokesperson.

      – The Honourable Mr Amador Sánchez Sánchez, Director General of Service Quality and Citizen's Advice of the Office of the Vice-President and the Government Spokesperson.

   c) The Local Authorities of the Madrid Region: two representatives assigned by the Federation of Madrid Municipalities.

      – The Honourable Mr Adolfo Rivas Morillo, Mayor of Orusco de Tajuña.

      – Mr Jorge Calderón Hernández, Town Councillor for San Sebastián de los Reyes.

   d) A representative from the trades unions organisations, elected by the Madrid Region Economic and Social Council.

      – Mr Daniel López Montesinos.

13. GENERAL SECRETARIAT

e) A representative from business organisations, elected by the Madrid Region Economic and Social Council.

– Mr Luís Méndez López.

f) An expert in the matter assigned by the Madrid Assembly.

– Mr Germán Alonso-Alegre Fernández de Valderrama.

2. To make an inventory of the assets and rights making up the Agency's heritage. At the 31 December the inventory comprised 844 assets valued at 666,407.32 €.

3. To notify the decisions of the Director of the Agency. In 2009 a total of 272 decisions were notified.

4. The dissemination of data and publications, including in particular, the report on the activities of the Agency, as well as the commissioning of the new institutional web and e-Publications of the agency.

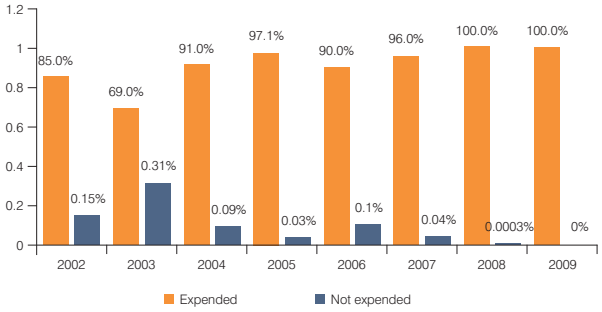
5. The management of the Agency's document collection, and particularly, compilation and updating of a document collection on legislation, case law and doctrine on issues of personal data protection and any related issue whatsoever. It should be underlined that the documentary collection of the Pablo Lucas Murillo de la Cueva Centre for Research and Documentation has increased.

6. To organise conferences, seminars, and data protection conferences in the Madrid Region, as well as collaborating with international or inter-regional cooperation actions that require the assistance of the Agency. The Secretary General has entrusted the organisation with all the conferences and events referred to in this report.

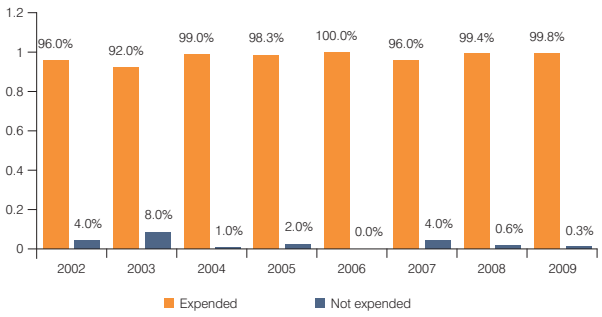
7. The institutional relations with various institutions to sign collaboration agreements as well as to study and edit their contents.

Regarding the financial management of the APDCM's budget for 2009, the high level of implementation reached this year should be pointed out, with 100% of the budget expenses allocated to this authority having been spent.

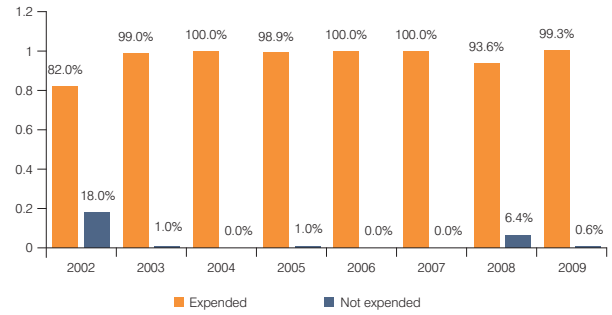
Budgetary Allocation I



Budgetary Allocation II



Budgetary Allocation VI



Total Program 125