

Prólogo	13
Abreviaturas	35

PRESENTACIONES

I. La tramitación administrativa del anteproyecto de Ley Orgánica de Protección de Datos de carácter personal.....	39
1. Introducción.....	39
2. Procedimiento administrativo de elaboración de la nueva normativa nacional de protección de datos	41
2.1. Elaboración, enfoque y contenido del primer anteproyecto	41
2.2. Participación ciudadana	48
2.3. Informes de las autoridades administrativas de protección de datos	54
2.4. Informes ministeriales.....	56
2.5. Informes del Consejo Fiscal y del Consejo General del Poder Judicial.....	59
2.6. Dictamen del Consejo de Estado.....	63
3. A modo de conclusión	67
II. El nuevo modelo europeo de protección de datos de carácter personal.....	69
III. España en la vanguardia de la Protección de Datos:nuevos retos del Reglamento Europeo.....	75
INTRODUCCIÓN. Un Reglamento poliédrico que necesita un acercamiento poliédrico	81
1. Introducción.....	81
2. Un reglamento que se justifica por su propia existencia como declaración de principios frente, principalmente, a Estados Unidos y sus empresas tecnológicas	84

2.1. Las tecnológicas como albaceas de la privacidad	85
2.2. Las tecnológicas son obligados por las autoridades a modular el alcance de la libertad de expresión.....	86
2.3. Adoptan objetivos limítrofes con el «servicio público»	88
2.4. «Legislan» en supuestos de vacío y lentitud	88
2.5. Avanzan hacia su independencia a través de sus propias líneas y encriptado.....	88
3. Los datos personales, principal víctima del principio de precaución en materia de seguridad	89
4. Una nueva forma de Derecho en la revolución tecnológica	90
4.1. Indicios de Common law en el derecho continental. La ascendente relevancia de la fase de implementación	91
4.2. La posible sobre-regulación en el ámbito comunitario como reacción a las amenazas extracomunitarias.....	92

PARTE 1

Perspectiva sectorial y específica

A) VALORACIONES SECTORIALES

CAPÍTULO I. Consideraciones de la Agencia Vasca de Protección de Datos	99
1. Incidencia del Reglamento General de Protección de Datos en las Administraciones Públicas. Consideraciones de la Agencia Vasca de Protección de Datos	99
2. Visión general.....	99
2.1. Fichero y Registro de Ficheros.....	100
2.2. Responsabilidad proactiva en las Administraciones Públicas	101
2.3. Cesiones de datos	103
2.4. Derechos de las personas.....	105
3. Papel de las autoridades de control y conciliación entre el derecho a la protección de datos y el derecho de acceso a la información pública	107
CAPÍTULO II. Una visión desde la judicatura	115
1. Introducción.....	115
2. Aplicación en España: Reglamento 2016/679 y Directiva 2016/680	115
2.1. Reglamento 2016/679.....	115
2.1.1. <i>La aplicabilidad directa</i>	117
2.1.2. <i>El efecto directo</i>	118
2.2. Directiva 2016/680.....	120
3. Ámbito civil	121
3.1. Autocomposición	121
3.2. Heterocomposición	122
3.3. Proceso civil.....	122
3.3.1. <i>Concepto</i>	122
3.3.2. <i>Publicidad</i>	123

A) Secreto	124
B) Reservado.....	125
C) Confidencial.....	126
D) La prueba	127
E) La sentencia	127
4. Ámbito penal.....	128
4.1. Diligencias a Prevención	128
4.1.1. Fase de reconocimiento	129
4.1.2. Fase de inicio.....	134
4.1.3. Fase de resolución	135
4.2. Diligencias de Investigación	137
4.3. Diligencias de Instrucción.....	139
4.4. Juicio oral	142
4.5. Fase de ejecución	143
5. Fuentes de Prueba	144
6. Modificaciones legislativas.....	145

CAPÍTULO III. El Reglamento General de Protección de Datos, y las Pymes.....

1. Sobre el concepto de microempresa, y pequeña y mediana empresa, y su régimen jurídico aplicable en materia de privacidad	147
2. Las cuestiones específicas sobre las microempresas, y las pequeñas y las medianas empresas, en la nueva normativa sobre Protección de Datos de Carácter Personal, establecidas sobre la base del nuevo Reglamento General	155
2.1. Los Códigos de Conducta.....	155
2.2. La obtención de certificaciones	158
3. La formación y la sensibilización de los responsables y encargados de tratamiento en el ámbito de la protección de datos	160
4. Otras cuestiones generales que afectan a las microempresas y a las pequeñas y medianas empresas en el nuevo Reglamento General de Protección de Datos	161

CAPÍTULO IV. El ciudadano frente al Reglamento

Introducción	163
1. El art. 18 de la Constitución.....	164
2. El art. 1 de la LOPD	164
3. El art. 1 del Reglamento	164
4. La Carta de los Derechos Fundamentales de la Unión Europea	165
5. Qué es un dato y cuántos tipos de datos hay	165
6. Qué es un dato personal.....	166
7. Qué NO es un dato personal	166
8. Qué es la identidad	167
9. De quién son los datos	167
10. Relaciones y correlaciones	167
11. ¿Titular o interesado?.....	168

12. Honor e imagen, intimidad y privacidad	168
13. Qué pueden hacer con mis datos	169
14. Consentimiento expreso.....	169
15. Interés público.....	169
16. Interés legítimo	170
17. Qué derechos tengo respecto a mis datos	170
18. Limitación del uso	171
19. Portabilidad de los datos.....	171
20. Qué puedo hacer si no se respetan mis derechos.....	172

CAPÍTULO V. Internet y el Reglamento General de Protección de Datos	173
1. Introducción.....	173
2. La privacidad en la economía de los datos	174
2.1. El valor de los datos	174
2.2. El seguimiento y perfilado de usuarios en los negocios de la economía digital	176
2.2.1. <i>Redes sociales</i>	176
2.2.2. <i>Dispositivos móviles</i>	179
2.2.3. <i>Big Data</i>	181
2.2.4. <i>Internet de las Cosas</i>	183
2.2.5. <i>Inteligencia artificial</i>	184
2.3. El fenómeno de los gigantes de internet o GAFAM	186
2.4. La perspectiva «user-centric» y los pasos hacia la regulación «patrimonialista» del derecho a la protección de los datos personales ...	188
3. Conclusiones	191

CAPÍTULO VI. Especialidades en el sector sanitario	195
1. Introducción.....	195
2. Datos de salud, datos genéticos y datos biométricos	196
2.1. Datos de Salud	196
2.2. Datos genéticos	198
2.3. Datos Biométricos	199
3. Marco regulatorio vigente	200
3.1. Marco Internacional y europeo	200
3.2. Derecho español.....	201
4. Incidencia de las novedades del Reglamento en materia de principios en relación con los datos de salud	203
4.1. Incidencia en relación con el principio de seguridad de los datos: la seudonimización de los datos.....	203
4.2. Los principios de responsabilidad proactiva de privacidad desde el diseño y por defecto en el tratamiento de los datos personales de relativos a la salud: la exigencia de realizar evaluación de Impacto	205
4.3. Límites a la elaboración de perfiles que contengan datos relacionados con la salud.....	207
4.4. La figura del delegado de protección de datos (DPO).....	208

5.	El requisito de consentimiento explícito para el tratamiento de los datos de salud: sus singularidades	209
5.1.	La importancia del consentimiento en el tratamiento de los datos de salud y su reflejo en la legislación española	209
5.2.	Los límites al principio de consentimiento del titular en materia de tratamiento de datos relativos a la salud, datos genéticos y biométricos	212
5.2.1.	<i>Regla general: necesidad de consentimiento</i>	212
5.2.2.	<i>Excepciones a la regla del consentimiento</i>	213
5.2.3.	<i>Tratamientos compatibles con el consentimiento inicial del interesado</i>	215
6.	Los derechos de acceso, rectificación, cancelación y oposición del titular del dato de salud: sus límites	216
6.1.	Principio general	216
6.2.	Especialidades con ocasión del ejercicio de derechos ARCO	216
6.2.1.	<i>En materia de derecho de acceso</i>	216
6.2.2.	<i>En materia de derecho de rectificación y supresión: límites al derecho al olvido</i>	217
7.	Cuestiones relacionadas con el tratamiento de datos para la investigación biomédica y farmacéutica	217
7.1.	Planteamiento general	217
7.2.	Tratamiento de datos personales procedentes de muestras biológicas	219
7.3.	Tratamiento de datos genéticos	220

B) ASPECTOS ESPECÍFICOS

CAPÍTULO VII. Redes sociales y aplicaciones móviles	223
1. Las redes sociales y el RGPD o el fruto de una relación complicada desde sus inicios	223
2. Un breve análisis histórico de las redes sociales	225
3. La aplicación de los principios generales de la normativa de protección de datos en las redes sociales	228
4. Aspectos referidos al deber de secreto y a los encargados de tratamiento: los «community managers»	237
5. RGPD y APPS	241
CAPÍTULO VIII. Cloud Computing	249
1. Y entonces apareció el «cloud computing»	249
2. Los datos en la red (punto de partida)	250
2.1. El uso y la custodia del dato	251
2.2. La deslocalización	251
2.3. Respecto al DATO y solo al dato personal	251
3. Cómo categorizamos el cloud	252
3.1. La seguridad, fiabilidad y resiliencia	255
4. Quién es el responsable del dato	256

4.1. El ciudadano	256
4.2. El cliente de servicios en la nube.....	257
4.3. El proveedor de servicios	257
4.3.1. La parte física, el IaaS.....	257
4.3.2. La base del PaaS.....	258
4.3.3. El prestador de SaaS.....	258
5. Qué podemos hacer.....	259
5.1. Normativa eficaz y armonización	259
5.2. Entorno procedimental y técnico	260
5.2.1. Privacidad por diseño	261
5.2.2. Privacidad por defecto	261
6. Cómo podemos controlar los niveles de seguridad.....	262
7. Y esto acaba de comenzar.....	263
7.1. Desde un punto de vista legal.....	263
7.2. Desde un punto de vista conceptual	264
CAPÍTULO IX. Cookies, fingerprinting y la privacidad digital	267
1. Contexto.....	267
1.1. La economía digital en datos y el papel de la publicidad digital...	267
1.2. Cookies. Definición y regulación	269
2. Las cookies y otras tecnologías en el Reglamento General de Protección de Datos y el Reglamento de e-Privacidad.....	270
3. Las cookies en la Propuesta de Reglamento de e-Privacidad	271
3.1. Consentimiento.....	272
3.2. Papel de los navegadores	273
3.3. Paredes de cookies (cookie walls)	274
3.4. Otras tecnologías: La huella digital (fingerprinting)	275
3.5. Personas físicas y jurídicas	276
4. Conclusiones	276
CAPÍTULO X. Consideraciones sobre el principio de responsabilidad proactiva y diligencia (accountability). Experiencias desde el compliance	279
1. Consideraciones sobre el principio de responsabilidad proactiva y diligencia (accountability)	279
2. Experiencias desde el compliance	285
CAPÍTULO XI. Inteligencia artificial y privacidad.....	289
1. Concepto de inteligencia artificial	289
2. Ventajas e inconvenientes	290
3. Reglamento General de Protección de Datos (en adelante RGPD) e inteligencia artificial.....	293
3.1. Decisiones automatizadas	293
3.2. Privacidad desde el diseño y evaluaciones de impacto.....	297
3.3. Nueva Ley Orgánica de Protección de Datos de Carácter Personal	297
4. Opinión de los reguladores.....	298

5. Autorregulación y otros medios.....	299
6. Conclusión.....	300

CAPÍTULO XII. La Internet de las Cosas y el Reglamento General de Protección de Datos	301
1. Introducción.....	301
1.1. Definición de Internet de las Cosas	301
1.2. Seguridad y privacidad.....	303
2. La privacidad y la Internet de las Cosas.....	305
2.1. Los retos para la protección de datos.....	305
2.2. Los principios generales de protección de datos	306
2.3. Consentimiento y otros fundamentos jurídicos para el tratamiento ...	307
2.4. La privacidad por defecto y desde el diseño	309
2.5. Evaluación de Impacto de la Protección de Datos (EIPD)	310
3. Conclusión.....	312

CAPÍTULO XIII. Blockchain y Protección de Datos.....	313
1. Introducción: una tecnología de vanguardia y en desarrollo	313
2. ¿Qué es blockchain?.....	318
3. ¿Cómo de seguro y anónimo es blockchain?	324
4. Aplicaciones de blockchain con relevancia sobre protección de datos personales.....	327
5. Conclusiones	331

PARTE 2

Análisis del articulado

CAPÍTULO XIV. Disposiciones Generales (Arts. 1-5)	335
1. Art. 1: Objeto	335
2. Art. 2: Ámbito de aplicación material	337
3. Art. 3: Ámbito territorial	339
4. Art. 4: Definiciones	340
5. Art. 5: Principios relativos al tratamiento.....	347
5.1. Licitud, lealtad y transparencia.....	347
5.2. Limitación de la finalidad.....	349
5.3. Minimización.....	349
5.4. Exactitud	349
5.5. Limitación del plazo de conservación	350
5.6. Integridad y confidencialidad	350
5.7. Responsabilidad proactiva	351

CAPÍTULO XV. Principios (Arts. 6-11)	353
1. Art. 6: Licitud del tratamiento	353
1.1. La licitud del tratamiento y el «interés legítimo»	353
1.2. Título IV del PROYECTO LOPD. Disposiciones aplicables a tratamientos concretos	355

2.	Art. 7: Condiciones para el consentimiento	357
2.1.	Cambio de paradigma en la prestación del consentimiento. Régimen transitorio para consentimientos previos.....	357
2.2.	Art. 6 del Proyecto LOPD. Tratamiento basado en el consentimiento del afectado	359
3.	Art. 8: condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información	359
4.	Art. 9: Tratamiento de categorías especiales de datos personales	360
4.1.	La protección de las categorías especiales de datos.....	360
5.	Art. 10: Tratamiento de datos personales relativos a condenas e infracciones penales	361
6.	Art. 11: Tratamiento que no requiere identificación	361
	CAPÍTULO XVI. Derechos del interesado (Arts. 12-19)	363
1.	El principio de transparencia	363
2.	Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado	367
2.1.	Carácter personalísimo de los derechos y autenticación del solicitante	368
2.2.	Deber de facilitar el ejercicio de los derechos.....	369
2.3.	Plazo para facilitar la información o rechazar la solicitud	370
2.4.	Canal para el ejercicio de los derechos y para facilitar la información. Gratuidad de la atención de los derechos.....	371
2.5.	Obligación de responder.....	376
2.6.	Uso de iconos informativos.....	376
3.	Información y acceso a los datos personales.....	377
3.1.	Deber de información	377
3.1.1.	<i>Información que deberá facilitarse cuando los datos personales se obtengan del interesado</i>	<i>379</i>
3.1.2.	<i>Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado</i>	<i>381</i>
3.1.3.	<i>Comparación de la información que debe aportarse en atención a su origen</i>	<i>383</i>
3.2.	Derecho de acceso del interesado	384
3.3.	Rectificación y supresión	388
3.3.1.	<i>Derecho de rectificación</i>	<i>388</i>
3.3.2.	<i>Derecho a completar el tratamiento</i>	<i>389</i>
3.3.3.	<i>Derecho de supresión</i>	<i>390</i>
3.3.4.	<i>Derecho al olvido</i>	<i>393</i>
3.3.5.	<i>Derecho al olvido frente a los motores de búsqueda.....</i>	<i>395</i>
3.3.6.	<i>Limitaciones al derecho de supresión y el derecho al olvido</i>	<i>397</i>
3.3.7.	<i>Derecho a la limitación del tratamiento</i>	<i>397</i>
	CAPÍTULO XVII. Derecho de portabilidad (Art. 20)	401
1.	Contextualizando el derecho a la portabilidad.....	401
2.	La regulación del derecho a la portabilidad	404

2.1. Datos afectados por el derecho a la portabilidad.....	404
2.2. Requisitos para ejercer el derecho a la portabilidad	405
2.3. Como deberán entregarse los datos.....	406
3. El derecho a la portabilidad en el proyecto de Ley Orgánica de Protección de Datos	407

CAPÍTULO XVIII. Derecho de oposición y decisiones individuales automatizadas. Limitaciones (Arts. 21-23).....

1. Derecho de oposición y decisiones individuales automatizadas.....	409
1.1. Derecho de oposición.....	409
1.2. Oposición al interés público e interés legítimo.....	410
1.3. Oposición a la finalidad de mercadotecnia directa	412
1.4. Eficacia de la oposición.....	412
1.5. Decisiones individuales automatizadas, incluida la elaboración de perfiles: big data.....	413
2. Limitaciones	416

CAPÍTULO XIX. Responsabilidad del responsable del tratamiento (Art. 24)

1. Introducción al concepto de Responsable y Responsabilidad.....	419
2. Análisis del art. 24.....	420
2.1. Apartado 1 (art. 24)	421
2.2. Apartado 2 (art. 24)	422
2.2.1. <i>Políticas internas</i>	423
2.2.2. <i>Políticas externas</i>	423
2.3. Apartado 3 (art. 24)	424
3. La Responsabilidad del Responsable en el Proyecto de Ley Orgánica de Protección de Datos.....	425

CAPÍTULO XX. Protección de datos desde el diseño y por defecto (Art. 25)

1. Contextualización de la protección de datos desde el diseño y por defecto.....	427
2. La protección de datos desde el diseño y por defecto.....	429
3. La protección de datos por defecto	431

CAPÍTULO XXI. El tratamiento y sus responsables (Arts. 26-29)

1. Contratos del reglamento (arts. 26 y 28).....	433
1.1. Contrato de corresponsables (art. 26).....	433
1.2. Contrato de tratamiento por cuenta del RT (art. 28 y 29)	437
1.2.1. <i>Descripción del tratamiento (art. 28.3 del Reglamento)</i>	437
1.2.2. <i>Medidas de seguridad (art. 28.b, c y e y art. 32 por referencia del Reglamento)</i>	438
1.2.3. <i>Subcontratación (arts. 28.2, 28.3.d y 28.4 del Reglamento)</i>	438
1.2.4. <i>Accountability (responsabilidad proactiva), cooperación y auditoría (art. 28.3.e, f y h del Reglamento)</i>	438

1.2.5. Finalización de los servicios (art. 28.3.g del Reglamento)	439
2. Representantes de RT y ET no establecidos en la UE (art. 27).....	440
2.1. Nombramiento del representante: regla general y excepciones	440
2.2. Establecimiento del representante	441
2.3. Funciones y responsabilidad del representante	441
CAPÍTULO XXII. Registro de actividades del tratamiento (Art. 30)	443
1. Introducción	443
2. ¿Quiénes estarán obligados a mantener el registro de actividades de tratamiento?	444
3. Contenido del Registro de Actividades de tratamiento, ¿cómo debemos gestionarlo?	445
3.1. Contenido del Registro de Actividades de tratamiento para los responsables del tratamiento	446
3.2. Contenido del Registro de Actividades de tratamiento para los Encargados	446
3.3. Otras consideraciones al Registro de Actividades de Tratamiento	448
4. «Relación» de actividades de tratamiento (no obligatoria pero muy recomendable)	448
5. El Registro de Actividades de tratamiento en el Proyecto LOPD	449
CAPÍTULO XXIII. Cooperación con la autoridad de control (Art. 31)...	451
CAPÍTULO XXIV. Seguridad del tratamiento (Art. 32).....	453
1. La perspectiva	453
2. ¡Bienvenido al país de la Reina Roja!	454
3. El Sistema de Gestión de la Seguridad de la Información.....	458
CAPÍTULO XXV. La obligación de notificar una violación de seguridad de datos personales (Arts. 33 y 34)	461
1. La obligación de notificación de la violación de seguridad a la autoridad de control.....	464
2. Notificación del responsable del tratamiento al interesado.....	466
2.1. El formato y contenido de la notificación.....	467
2.2. La obligación de notificación de incidentes en la Directiva NIS..	469
CAPÍTULO XXVI. Evaluación de impacto relativa a la protección de datos y consulta previa (Arts. 35 y 36)	471
1. Introducción a la evaluación de impacto relativa a la protección de datos	471
2. La regulación de la evaluación de impacto relativa a la protección de datos	472
2.1. Art. 35 del Reglamento: evaluación de impacto relativa a la protección de datos.....	474
2.1.1. Supuestos en que deberá realizarse la evaluación de impacto.....	475
2.1.2. El obligado a hacer la evaluación de impacto	477

2.1.3. Contenido mínimo de la evaluación de impacto.....	478
2.1.4. Potenciales infracciones relacionadas con las evaluaciones de impacto	481
2.1.5. Revisión de la evaluación de impacto.....	482
2.1.6. La consulta a las partes afectadas en una evaluación de impacto .	483
2.1.7. El delegado de protección de datos y las evaluaciones de impacto .	483
3. Los conceptos de «alto riesgo» y a «gran escala».....	484
3.1. El «alto riesgo» en el contexto de las evaluaciones de impacto	484
3.2. El concepto de «a gran escala» en el contexto de las evaluaciones de impacto	487
4. Aspectos metodológicos de las evaluaciones de impacto	488
5. Regulación de la consulta previa	490

CAPÍTULO XXVII. El Delegado de Protección de Datos: Guardián de la Privacidad (Arts. 37, 38 y 39).....

1. Introducción.....	493
2. ¿Qué es un Delegado de Protección de Datos?.....	494
3. ¿Quién no es un DPD?	496
3.1. Personal específico de protección de datos o Consultores externos ...	496
3.2. Comité de protección de datos.....	497
3.3. Relacionadas con la seguridad de la información: Responsable de seguridad, CSO, CPO o CISO	497
3.4. Relacionadas con la gestión de la información: CDO y CIO	498
3.5. El Compliance Officer o el Director de Cumplimiento Normativo..	499
3.6. Otras figuras en las administraciones públicas.....	499
4. Su perfil profesional	500
4.1. Formación exigida.....	500
4.2. Independencia.....	501
4.3. Conflicto de interés	502
4.4. Certificación profesional.....	502
4.5. Ética	504
4.5.1. Principios generales.....	504
4.5.2. En sus relaciones con el resto de empleados, directivos y colaboradores de la organización	504
4.5.3. En sus relaciones con los colaboradores externos y proveedores....	505
4.5.4. En sus relaciones con los clientes/usuarios	505
4.5.5. Relaciones con terceros	505
4.5.6. Desempeño de otras actividades profesionales.....	506
4.5.7. Incumplimiento	506
4.6. El deber de secreto	506
4.7. Capacidades	506
5. Las funciones del DPD.....	508
5.1. Informar y asesorar	509
5.2. Supervisar el cumplimiento	509
5.2.1. De las políticas.....	510
5.2.2. De la asignación de responsabilidades	511
5.2.3. De la concienciación	511

5.2.4. De la formación.....	511
5.2.5. De las auditorías	512
5.3. Asesoramiento sobre la evaluación de impacto relativa a la protección de datos.....	512
5.4. Cooperar con la autoridad de control	513
5.5. Punto de contacto con la autoridad de control.....	512
5.6. La resolución de quejas de los interesados	513
6. Las tareas requeridas.....	514
6.1. Explícitas	514
6.2. Implícitas	517
6.3. La triple visión de la actividad del DPD, jurídica, organizativa y tecnológica.....	518
7. ¿Quién debe designar un DPD?	520
7.1. Cuando el tratamiento lo lleve a cabo una autoridad u organismo público.....	520
7.2. En casos de observación habitual y sistemática de interesados a gran escala.....	522
7.3. Tratamiento a gran escala de categorías especiales de datos	525
7.4. Otros casos	525
7.5. Las ventajas de contar con un DPD	527
7.6. ¿Cuándo nombrarlo?	529
7.7. Fin de las funciones del DPD.....	530
7.8. Comunicación a las autoridades de control	530
7.9. Publicación de los datos de contacto del DPD	531
8. ¿Cómo seleccionar un DPD para nuestra organización?.....	531
8.1. Cualificación profesional.....	533
8.2. Interno o externo.....	533
8.3. Unipersonal o equipo	535
9. Posición en la organización	535
10. Ubicación física	537
11. Repercusiones de las actuaciones del DPD.....	538
11.1. ¿Cuál es la responsabilidad del DPD?.....	538
11.2. Costes de sus errores.....	538
12. Guía práctica para DPDs	539
12.1. Prepárate para el nuevo Régimen de Protección de Datos.....	539
12.2. Capacitación, formación y su acreditación	541
12.3. Retos. Algunos de los problemas que nos podemos encontrar siendo DPD	542
CAPÍTULO XXVIII. Los códigos de conducta y las certificaciones en el reglamento europeo de protección de datos (Arts. 40-43)	545
1. Introducción.....	545
2. Los códigos de conducta (arts. 40 y 41).....	546
2.1. ¿Quiénes pueden promover un código de conducta?.....	546
2.2. Contenido mínimo.....	546
2.2.1. La seudonimización	548

2.2.2. La notificación de violaciones de la seguridad de los datos personales a las autoridades de control y su comunicación a los interesados	551
2.3. Aprobación del código de conducta	552
2.4. Supervisión de los códigos de conducta	553
2.4.1. ¿Quién podrá ser órgano supervisor?	553
2.4.2. ¿Qué debe entenderse por medidas oportunas? ¿Puede el órgano supervisor crear esas medidas?	554
2.4.3. Responsabilidad del órgano supervisor	555
2.5. ¿Por qué los códigos de conducta no han sido atractivos en España? ...	555
2.6. ¿Qué hacer para conseguir impulsar la adhesión de las empresas españolas a los Códigos de Conducta?	556
3. Las certificaciones (arts. 42 y 43).....	559

CAPÍTULO XXIX. Transferencias de Datos Personales a terceros países y organizaciones internacionales (Arts. 44-50).....

1. Introducción (art. 44).....	563
2. Nivel adecuado de protección (art. 45).....	566
2.1. ¿Qué es un nivel adecuado de protección?.....	566
2.1.1. Principios de contenido	567
2.1.2. Mecanismos de procedimiento/aplicación.....	569
2.2. Determinación del nivel adecuado: «lista blanca», especial referencia al difunto Safe Harbor y actual Privacy Shield	570
2.2.1. Lista blanca	570
2.2.2. Especial referencia al difunto Safe Harbor y actual Privacy Shield ..	572
3. Garantías (arts. 46 y 47).....	576
3.1. Consideraciones generales.....	576
3.2. Garantías específicas.....	577
3.2.1. Cláusulas contractuales tipo (CCT).....	577
3.2.2. Las normas corporativas vinculantes	579
3.2.3. Códigos de conducta y certificaciones.....	583
4. Excepciones (art. 49).....	585
4.1. Consideraciones generales.....	585
4.2. Excepciones específicas.....	586
4.2.1. Sector público.....	586
4.2.2. Consentimiento	586
4.2.3. Interés público.....	587
4.2.4. Interés legítimo.....	588
5. Decisiones administrativas o judiciales de país tercero (art. 48)	588
6. Cooperación internacional (art. 50)	590

CAPÍTULO XXX. Autoridades de control independientes (Arts. 51-59)

1. Art. 51: Autoridad de control.....	591
2. Art. 52: Independencia	593
3. Art. 53: Condiciones generales aplicables a los miembros de la autoridad de control y art. 54. Normas relativas al establecimiento de la autoridad de control.....	595

4.	Art. 55: Competencia	597
5.	Art. 56: Competencia de la autoridad de control principal	597
6.	Art. 57: Funciones.....	601
7.	Art. 58: Poderes.....	603
8.	Art. 59: Informe de actividad	607
CAPÍTULO XXXI. Cooperación y coherencia (Arts. 60-76)		609
1.	La coexistencia de medidas centralizadoras y descentralizadoras.....	609
2.	Algunos rasgos esenciales del sistema de cooperación y coherencia	610
2.1.	Vertiente decisoria	611
2.2.	Vertiente consultiva	612
3.	La autoridad de control principal como pilar del sistema	615
3.1.	Sobre las empresas	615
3.2.	Sobre los ciudadanos:.....	616
4.	Fase primera: mecanismo de cooperación.....	617
4.1.	Principios.....	617
4.2.	Asistencia mutua.....	618
4.3.	Operaciones conjuntas.....	619
5.	Segunda fase. Mecanismo de coherencia: en caso de desacuerdo o requerimiento de dictamen.....	621
6.	Resolución de conflictos por el comité: supuestos, requisitos y autoridad que realiza la adopción	623
7.	Procedimiento de urgencia: medidas provisiones, inacción	624
8.	Comité europeo de protección de datos.....	624
8.1.	Régimen y funcionamiento	624
8.2.	Organización	625
8.3.	Recursos directos e indirectos frente a sus resoluciones	627
8.4.	Peculiaridades de la coexistencia de la AEPD con autoridades autonómicas.....	628
8.5.	Funciones del Comité.....	629
8.5.1.	<i>Promoción</i>	630
8.5.2.	<i>Asesoramiento</i>	630
8.5.3.	<i>Emisión de directrices</i>	630
8.5.4.	<i>Control de la implementación</i>	631
8.5.5.	<i>Llevanza de un registro público</i>	631
8.5.6.	<i>Elaboración de un informe anual</i>	631
CAPÍTULO XXXII. Recursos, responsabilidad y sanciones (arts. 77-84)....		633
1.	Recursos, responsabilidad y sanciones: claves del nuevo enfoque legal contenido en el RGPD	633
2.	El régimen jurídico relativo a los recursos dentro del marco europeo regulador de la protección de los datos personales	635
2.1.	Introducción	635
2.2.	La representación de los interesados.....	638
2.3.	El derecho a presentar una reclamación ante una autoridad de control.....	640

2.4. El derecho a la tutela judicial efectiva contra una autoridad de control.....	646
2.5. El derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento	648
3. Pendencia y suspensión de los procedimientos.....	648
4. Derecho a indemnización y responsabilidad	649
5. Las Sanciones. Especial consideración de la imposición de multas administrativas en el RGPD.....	652
5.1. Consideraciones generales.....	652
5.2. El Régimen Jurídico Sancionador	656
5.2.1. <i>Personas o sujetos responsables</i>	656
5.2.2. <i>Infracciones</i>	656
5.2.2.1. <i>Infracciones muy graves</i>	656
5.2.2.2. <i>Infracciones menos graves</i>	657
5.2.2.3. <i>Infracciones consideradas muy graves</i>	657
5.2.2.4. <i>Infracciones consideradas graves</i>	658
5.2.2.5. <i>Infracciones consideradas leves</i>	660
5.2.3. <i>Plazos de prescripción de las infracciones e interrupción de la misma</i> ..	662
5.2.4. <i>Sanciones y medidas coercitivas</i>	662
5.2.4.1. <i>Tipos de sanciones</i>	662
5.2.4.2. <i>Las multas administrativas: condiciones y criterios para su imposición</i>	663
5.2.4.3. <i>Multas administrativas a autoridades y organismos públicos</i>	664
5.2.4.4. <i>Supuestos de publicación de las sanciones en el Boletín Oficial del Estado según el proyecto de LOPD</i>	665
5.2.4.5. <i>Prescripción de sanciones</i>	665
5.2.5. <i>El mecanismo del apercibimiento</i>	665
5.3. Tratamiento de datos relativos a infracciones y sanciones administrativas	667
6. Consideraciones finales	667

CAPÍTULO XXXIII. Disposiciones relativas a situaciones específicas de tratamiento (Arts. 85-91).	671
1. Las situaciones específicas de tratamiento	671
2. Tratamiento de datos y libertad de expresión e información	672
2.1. El conflicto histórico entre los tratamientos de datos y las libertades informativas.....	672
2.2. La situación española en cuanto la regulación normativa	673
3. Tratamiento y acceso del público a documentos oficiales	681
4. Tratamiento del número nacional de identificación	684
5. Tratamiento en el ámbito laboral	685
6. Tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.....	691
6.1. El principio de limitación con eje vertebrador del art. 89 del Reglamento	691

6.2. Tratamientos referidos a la función estadística pública	693
6.3. Tratamientos de datos con fines de archivo en interés público.....	695
6.4. Tratamientos en investigación científica y técnica.....	696
7. Obligaciones de secreto.....	697
8. Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas.....	697

CAPÍTULO XXXIV. Actos delegados y actos de ejecución. Disposiciones finales (Arts. 92-99)	703
1. Objeto y definiciones.....	703
1.1. Aplicación del art. 290 del TFUE: «actos delegados»	704
1.2. Aplicación del art. 291 del TFUE: «actos de ejecución».....	705
2. Consideraciones al Reglamento General de Protección de Datos.....	707
2.1. El ejercicio de la Delegación y el procedimiento de Comité.....	708
2.2. Relación con la Directiva 2002/58/CE	709
3. Conclusiones	711
3.1. Actos delegados y de ejecución	711
3.2. Directiva sobre privacidad y comunicaciones electrónicas.....	712

PARTE 3

Adaptación al reglamento. Experiencias prácticas

CAPÍTULO XXXV. La adaptación de los consentimientos tácitos y presuntos: el uso del interés legítimo	717
1. Introducción.....	717
2. El consentimiento en la antigua LOPD.....	720
3. El consentimiento en el Reglamento: el interés legítimo como sanador de consentimientos no expresos.....	722
4. ¿Cómo aplicar el interés legítimo? El dictamen 6/2014 del GT29.....	727
4.1. Ponderación entre el interés legítimo y los intereses o derechos y libertades de los interesados.....	729
4.2. El equilibrio provisional.....	729
4.3. Garantías adicionales.....	730
4.4. Equilibrio final.....	730

CAPÍTULO XXXVI. Adaptación al reglamento. Una experiencia práctica	735
1. Introducción de una experiencia práctica. Revisión e implantación de políticas de protección de datos	735
2. ¿Cómo dimensionar un proyecto y que recursos emplear durante el desarrollo?.....	736
3. Fase previa al inicio del proyecto	736
3.1. ¿Cómo determinar el alcance de un proyecto?	737
3.1.1. Entender el entorno en el que nos movemos	737
3.1.2. Conocimiento de la estructura organizativa y funcional de la organización.....	738

3.1.3. <i>En relación con la actividad principal, es importante que conozcamos el marco normativo en el que nos vamos a mover.....</i>	738
3.2. ¿Qué se solicitó? y ¿qué se aportó en nuestro caso particular?	738
4. Fase I: Inicio del proyecto.....	739
5. Fase II: Análisis de situación y metodología	739
6. Desarrollo de la Fase II.....	740
6.1. Análisis de situación respecto de los tratamientos y las partes que intervienen en el mismo	740
6.2. Análisis/Evaluación de los Riesgos	741
7. Fase III: Plan de acción	744
8. Fase IV: Verificación	745
9. Fase V: Asesoramiento continuado y mejora continua (opcional)	745
CAPÍTULO XXXVII. Claves prácticas para adaptarse al RGPD	747
1. Antes de empezar. Cuestiones previas a considerar.....	747
1.1. Estado de partida y estado de cumplimiento actual de la LOPD..	747
1.2. Contexto de la organización	747
1.3. Tipo de organización.....	748
1.4. Fijación de objetivos.....	748
1.4.1. <i>Objetivos realistas y alcanzables</i>	<i>748</i>
1.4.2. <i>Objetivos a corto, medio y largo plazo.....</i>	<i>748</i>
1.5. Dedicación de recursos	749
1.5.1. <i>La dedicación de personas</i>	<i>749</i>
1.5.2. <i>Los recursos tecnológicos</i>	<i>750</i>
2. El proceso de Adecuación al RGPD	750
2.1. Fase 1: Diagnóstico y Análisis GAP.....	750
2.2. Fase 2: Plan de Acción	751
2.3. Fase 3: Implantación de medidas RGPD	753
2.3.1. <i>DPO y Gobierno de la Privacidad</i>	<i>753</i>
2.3.2. <i>Inventario de tratamientos y finalidades.....</i>	<i>753</i>
2.3.3. <i>Consentimientos y cláusulas de información.....</i>	<i>754</i>
2.3.4. <i>Derechos de los interesados.....</i>	<i>755</i>
2.3.5. <i>Privacy by Design y Privacy by Default</i>	<i>756</i>
2.4. Fase 4: Concienciación y cultura de privacidad	758
Concordancias de los artículos del RGPD con sus considerandos	761