

ÍNDICE SISTEMÁTICO

ABREVIATURAS	19
INTRODUCCIÓN	23
PRIMERA PARTE. DESIGNAR A UN DELEGADO DE PROTECCIÓN DE DATOS	27
I. SUPUESTOS DE DESIGNACIÓN	30
1. ¿Quién debe designarlo?	30
2. Supuestos de designación	33
2.1. Designación obligatoria	33
2.1.1. Autoridad u organismo público	33
2.1.2. Observación habitual y sistemática de intereses a gran escala	36
2.1.3. Tratamiento a gran escala de categorías especiales de datos	41
2.1.4. Supuestos establecidos en la LOPDGDD ..	42
2.2. Designación voluntaria	44
3. Designación de un DPD para varias organizaciones	47
4. Designación a cargo del encargado del tratamiento.	50
5. Formalizar la designación	52
II. CARACTERÍSTICAS QUE DEBE REUNIR ESTE PERFIL	54
1. ¿Quién puede ser DPD?	54
1.1. Persona física, jurídica u órgano colegiado	54
1.2. Personal interno o contratación externa	56
2. Criterios para la selección de un DPD	59
2.1. Conocimientos	59
2.2. Experiencia	60
2.3. Capacidades	61
3. Certificaciones	62
III. POSICIÓN DENTRO DE LA ORGANIZACIÓN	67
1. Independencia	67
1.1. Operativa o total	68

1.2.	Reportar al más alto nivel jerárquico	71
1.3.	Imposibilidad de sanción o destitución	73
1.4.	Conflicto de intereses.	75
1.5.	Secreto y confidencialidad.	78
2.	Participación en las cuestiones relativas a la protección de datos.	79
3.	Asignación de recursos suficientes.	81
3.1.	Apoyo de la organización	81
3.2.	Formación	83
3.3.	Tiempo	84
3.4.	Recursos económicos o materiales.	84
3.5.	Recursos humanos.	85
3.6.	Acceso a los datos y operaciones de tratamiento	85
IV.	FUNCIONES	86
1.	Informar y asesorar	87
2.	Supervisar	90
3.	Cooperar con la autoridad de control	93
4.	Actuar como punto de contacto.	95
V.	RESPONSABILIDAD	97
VI.	FIGURAS AFINES	99
1.	Responsables de la adecuación a la normativa	99
2.	<i>Compliance Officer</i>	100
3.	Representante del responsable o del encargado.	106
4.	Responsable de seguridad	108
4.1.	Responsable de seguridad LOPD.	108
4.2.	Responsable de seguridad del Esquema Nacional de Seguridad.	109
SEGUNDA PARTE. MANUAL PARA EL DELEGADO DE PROTECCIÓN DE DATOS		111
I.	CONCEPTOS BÁSICOS.	114
1.	Análisis en clave de derechos fundamentales y determinación de la normativa aplicable.	114
1.1.	Análisis en clave de derechos fundamentales.	114
1.1.1.	Los orígenes del derecho	115
1.1.2.	El origen europeo de la regulación del derecho en el marco del Consejo de Europa	120
1.1.3.	El reconocimiento del derecho en la Carta de derechos fundamentales de la Unión Europea	122
1.1.4.	El derecho en el ordenamiento jurídico español	125

1.1.5.	Límites al derecho a la protección de datos	127
1.2.	Determinación de la normativa aplicable	129
1.2.1.	El Reglamento General de Protección de Datos	129
1.2.2.	La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales	133
1.2.3.	Normativa autonómica	135
a.	Cataluña	136
b.	País Vasco	138
c.	Andalucía	138
1.2.4.	Normativa especial	139
1.2.5.	Normativa relativa a datos no personales	140
2.	Ámbito de aplicación	142
2.1.	Ámbito objetivo	143
2.1.1.	Del concepto de fichero al de tratamiento	143
a.	Fichero	143
b.	Tratamiento	150
2.1.2.	Datos personales	153
a.	Toda información	154
b.	Sobre	156
c.	(Persona) Identificada o identificable	159
d.	Persona física	170
e.	Categorías especiales de datos	171
2.1.3.	Exclusiones	171
a.	Personas jurídicas	171
b.	Personas fallecidas	172
c.	Tratamientos a los que no se aplique el Derecho de la Unión y los relativos a la política exterior y de seguridad común	174
d.	Tratamientos con fines penales	177
e.	Tratamientos efectuados en el ejercicio de actividades personales o domésticas	177
2.2.	Ámbito subjetivo	181
2.2.1.	Responsable del tratamiento	182
a.	Características del concepto	182
b.	Los elementos del concepto	183
c.	Corresponsables	191
2.2.2.	Encargado del Tratamiento	200
a.	La definición de encargado del tratamiento	200

	b. La distinción entre el encargado y el responsable	206
	2.2.3. Representante	208
	2.2.4. Destinatario	211
	2.3. Ámbito territorial	215
	2.3.1. El criterio relativo al establecimiento	217
	2.3.2. El criterio relativo al <i>targeting</i>	220
	2.3.3. El criterio de aplicación del derecho internacional público	225
II.	PRINCIPIOS	226
	1. Principios relativos al tratamiento	226
	2. Principio de licitud	227
	2.1. La elección de la base jurídica	228
	2.2. Consentimiento	230
	2.2.1. Elementos del consentimiento	230
	a. Libre	230
	b. Específico	234
	c. Informado	234
	d. Inequívoco	236
	2.2.2. Condiciones adicionales del consentimiento	238
	a. Demostrar que se consintió	238
	b. Retirada del consentimiento	239
	2.2.3. Especial protección de los menores	240
	2.2.4. Tratamiento con fines de investigación	242
	2.3. Ejecución de contrato	244
	2.3.1. Ejecución de contrato	244
	2.3.2. Aplicación de medidas precontractuales	245
	2.4. Obligación legal	245
	2.5. Interés vital	249
	2.6. Misión realizada en interés público o en ejercicio de poderes públicos	250
	2.6.1. La necesidad de un fundamento legal	250
	2.6.2. La necesidad de incorporar el interés legítimo de las administraciones	251
	2.6.3. Los supuestos previstos en la LOPDGDD	253
	2.7. Interés legítimo	254
	2.7.1. El análisis del GA29	254
	a. Fase 1: Identificación de la base jurídica aplicable	255
	b. Fase 2: Existencia de un interés legítimo	255

	c.	Fase 3: Determinar si el tratamiento es necesario para conseguir el interés perseguido	257
	d.	Fase 4: Realizar una ponderación inicial en la que se establezca si los intereses del responsable prevalecen sobre los intereses y derechos de los interesados	258
	e.	Fase 5: Ponderación final teniendo en cuenta las medidas adicionales aplicadas por el responsable del tratamiento	263
	f.	Fase 6: Demostrar el cumplimiento y garantizar la transparencia	264
	g.	Fase 7: Ejercicio del derecho de oposición	264
	2.7.2.	Supuestos en los que se presume la prevalencia del interés legítimo del responsable	265
	a.	Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales	267
	b.	Sistemas de información crediticia	269
	c.	Tratamientos relacionados con la realización de determinadas operaciones mercantiles.	271
	2.8.	Tratamiento de categorías especiales de datos	272
	2.8.1.	La prohibición general y sus excepciones.	272
	2.8.2.	Una referencia al consentimiento explícito.	277
	2.9.	Tratamiento de datos relativos a condenas e infracciones penales.	279
	2.10.	Tratamiento que no requiere identificación	280
	3.	Lealtad y transparencia	281
	4.	Limitación de la finalidad	284
	4.1.	Bases jurídicas habilitadas	285
	4.2.	Determinación de la compatibilidad del tratamiento ulterior.	287
	5.	Minimización de datos	289
	6.	Exactitud	290
	7.	Limitación del plazo de conservación	291
	8.	Integridad y confidencialidad	292
	9.	Responsabilidad proactiva.	293
III.	DERECHOS		296
	1.	Información	296
	1.1.	Contenido de la información	296

1.1.1.	Recogida directa	297
1.1.2.	Recogida indirecta	299
1.1.3.	Tratamiento ulterior	303
1.2.	Metodología para proporcionar la información	304
2.	Acceso	309
2.1.	Contenido de la información a la que se puede tener acceso	310
2.2.	Cómo debe facilitarse el acceso	310
3.	Rectificación	313
4.	Supresión (derecho al olvido)	315
4.1.	El derecho de supresión	316
4.2.	El derecho al olvido digital	316
4.3.	Excepciones	320
4.4.	El derecho al olvido en la LOPDGDD	323
5.	Limitación del tratamiento	325
6.	Portabilidad	326
6.1.	¿A qué datos se refiere el derecho a la portabilidad?	327
6.2.	¿Cómo debe transmitirse la información?	328
6.3.	Responsabilidad	330
6.4.	El derecho a la portabilidad en la LOPDGDD	331
7.	Oposición	332
8.	Decisiones individuales automatizadas, incluida la elaboración de perfiles	333
8.1.	Elaboración de perfiles	334
8.2.	Decisiones individuales automatizadas, incluida la elaboración de perfiles	335
8.3.	Relación con otros derechos del interesado	337
9.	Ejercicio de los derechos	338
9.1.	Identificación del interesado que realiza la solicitud y representación	339
9.2.	Plazos para responder	340
9.3.	Medios y gratuidad	340
9.4.	Actuaciones posteriores al ejercicio	341
10.	Limitaciones	342
IV.	OBLIGACIONES	343
1.	Obligaciones que regulan la relación entre sujetos obligados	344
1.1.	Corresponsabilidad	344
1.2.	Encargado del tratamiento	346
1.2.1.	La relación contractual entre responsable y encargado del tratamiento	347
1.2.2.	Obligaciones asignadas al encargado del tratamiento derivadas del artículo 28 RGPD	349

	a.	Ofrecer garantías suficientes.	349
	b.	Seguir las instrucciones del responsable	349
	c.	Deber de confidencialidad	350
	d.	Medidas de seguridad.	350
	e.	Subcontratación	351
	f.	Supresión o devolución de los datos.	351
	g.	Poner a disposición del responsable la información que demuestra el cumplimiento de sus obligaciones.	352
	h.	Deberes de asistencia al responsable del tratamiento	352
	1.3.	Tratamiento bajo la autoridad del responsable o del encargado del tratamiento	352
2.		Obligaciones del responsable y del encargado	354
	2.1.	Responsabilidad.	354
	2.1.1.	Sujetos obligados	355
	2.1.2.	Las medidas	356
	2.1.3.	Demostrar	359
	2.1.4.	Metodología: enfoque de riesgos y sistemas de gestión de cumplimiento	360
	a.	Enfoque de riesgos	360
	b.	Sistemas de gestión de cumplimiento	363
	2.2.	Protección de datos desde el diseño y por defecto	368
	2.3.	Registro de las actividades de tratamiento	372
	2.4.	Seguridad.	376
	2.4.1.	Seguridad del tratamiento.	377
	a.	La evolución del nivel de madurez respecto a la obligación de seguridad de la Directiva 95/46/CE al RGPD	377
	b.	La seguridad en el RGPD y en la LOPDGDD: ¿un mayor nivel de madurez?	380
	c.	Análisis de los elementos del artículo 32 RGPD	382
	2.4.2.	Notificación y comunicación de violaciones de seguridad de datos personales	386
	a.	Concepto de violación de seguridad de datos personales	388
	b.	Sujetos obligados	389
	c.	Notificación a la autoridad de control	391
	d.	Comunicación a los interesados	395
	e.	Evaluación de riesgos	397

	f.	Documentación	398
	g.	Otras normativas que obligan a la notificación de incidentes de seguridad	399
	2.5.	Evaluación de impacto relativa a la protección de datos	400
	2.5.1.	Sujetos obligados	401
	2.5.2.	Supuestos en los que debe realizarse	403
	2.5.3.	¿Cómo debe realizarse?	410
	a.	Análisis preliminar	410
	b.	Descripción sistemática del tratamiento	411
	c.	Evaluación de la necesidad y la proporcionalidad.	412
	d.	Identificación de las medidas ya previstas para cumplir con el RGPD	413
	e.	Evaluación de riesgos para los derechos y libertades.	413
	f.	Medidas para afrontar los riesgos	414
	g.	Documentación	414
	h.	Supervisión y revisión.	415
	i.	Consulta de las partes interesadas.	415
	2.6.	Consulta previa	416
	3.	El bloqueo	418
V.		TRANSFERENCIAS.	420
	1.	Principio general	421
	2.	Decisión sobre la adecuación del nivel de protección de los datos	423
	3.	Garantías adecuadas	429
	4.	Excepciones.	431
	4.1.	Consentimiento explícito.	433
	4.2.	Ejecución de un contrato entre el interesado y el responsable del tratamiento o de medidas precontractuales	435
	4.3.	Celebración o ejecución de un contrato, en interés del interesado	436
	4.4.	Razones importantes de interés público.	437
	4.5.	Formulación, ejercicio o defensa de reclamaciones.	438
	4.6.	Protección de los intereses vitales del interesado o de otras personas.	438
	4.7.	Registro público.	439
	4.8.	Interés legítimo imperioso	440
	5.	Transferencias o comunicaciones no autorizadas por el derecho de la Unión	442

VI. CÓDIGOS DE CONDUCTA Y CERTIFICACIÓN	443
1. Una clara apuesta por la autorregulación regulada como corolario de la responsabilidad proactiva.	443
2. Códigos de conducta.	445
2.1. Concepto y contenido del código	445
2.2. Aprobación de los códigos.	447
2.3. El organismo de supervisión.	448
3. La certificación	449
3.1. Concepto y mecanismos	449
3.2. Procedimiento de certificación	450
3.3. Órganos de certificación	451
ANEXO	453
BIBLIOGRAFÍA	459
DOCUMENTACIÓN	463

