

© Autoras
© CEMCI Publicaciones
Plaza Mariana Pineda, 8. 18009-Granada
www.cemci.org
publicaciones@cemci.org

ISBN: 978-84-16219-46-9
Depósito legal: GR-802-2021

Impreso: Imprenta Diputación de Granada
Impreso en España - Printed in Spain

El editor no se hace responsable de las opiniones expresadas por
sus colaboradores.



ÍNDICE

Presentación	17
Prólogo	21
Acrónimos	25
CAPÍTULO PRIMERO. LEGISLACIÓN APLICABLE.....	27
1. Introducción: marco normativo en materia de protección de datos.....	29
2. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE.....	34
3. Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.....	57
4. Objetivos para la adaptación al RGPD y LOPDGDD para las entidades locales	63
5. ¿Está derogada la LOPD (Ley Orgánica 15/1999) y su Reglamento de desarrollo RD 1720/2007?	65

CAPÍTULO SEGUNDO. PRINCIPIOS Y CONCEPTOS BÁSICOS EN LA NORMATIVA DE PROTECCIÓN DE DATOS ...	69
1. Principios que legitiman el tratamiento de los datos	71
2. Datos de carácter personal	80
3. Categorías especiales de datos.....	92
4. Aplicabilidad: excepciones.....	97
5. Tratamiento.....	101
CAPÍTULO TERCERO. FIGURAS INTERVINIENTES	105
1. Responsable del tratamiento	107
1.1. Normativa que desarrolla la obligación	107
1.2. ¿Quién asume el rol de responsable de tratamiento?	108
1.3. Principales obligaciones del Responsable de Tratamiento.....	109
2. Corresponsables del tratamiento.....	111
3. Encargado de tratamiento.....	116
3.1. Normativa que desarrolla la figura	116
3.2. La definición del encargado de tratamiento y las obligaciones propias de los encargados.....	118
3.3. Las garantías que debe aportar el encargado de tratamiento.....	120
3.4. Relación entre responsable y encargado de tratamiento, Contrato de encargado de tratamiento	124
3.5. Encargado del tratamiento en virtud de competencias.....	128
3.6. ¿El encargado de tratamiento de una administración puede llegar a ser responsable de tratamiento?	129
3.7. Contrato de encargado de tratamiento firmados con antelación a la plena aplicación del RGPD.....	129
3.8. Conclusiones	130

4. Autoridades de control.....	131
4.1. Normativa que la desarrolla y definiciones.....	131
4.2. Agencia Española de Protección de Datos	132
4.3. Autoridades autonómicas	135
5. Delegado de protección de datos o DPD	136
5.1. Normativa que desarrolla la obligación	136
5.2. Nombramiento del delegado de protección de datos.....	138
5.3. Capacitación.....	138
5.4. Posición	138
5.5. Funciones	139

**CAPÍTULO CUARTO. EL REGISTRO DE
ACTIVIDADES DE TRATAMIENTO**

Registro de actividades y su publicación por medios electrónicos	145
1. Actuaciones para identificar las actividades de tratamiento	147
2. Publicación del registro de actividades, por medios electrónicos	150
3. Aspectos prácticos sobre el trabajo de obtención del registro de actividades.....	152
4. Referencia a algunos tratamientos.....	153
4.1. El tratamiento de las denuncias anónimas	153
4.2. Tratamiento de datos con fines de archivo en interés público por parte de las administraciones públicas.....	165
4.3. Tratamiento de datos de personas fallecidas	168
4.4. Tratamientos sometidos a la Directiva (UE) 2016/680 prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales y a la Ley	

Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales..... 171

CAPÍTULO QUINTO. TRANSPARENCIA, EJERCICIO DE DERECHOS, BRECHAS DE SEGURIDAD..... 187

1. Cumplimiento del principio de transparencia en el tratamiento de datos de carácter personal.....	189
1.1. Normativa de aplicación.....	189
1.2. Información que se debe facilitar y forma de hacerlo	190
1.3. Aspectos prácticos sobre el deber de transparencia.....	195
2. Atención al ejercicio de derechos de las personas afectadas.....	195
2.1. Normativa de aplicación.....	195
2.2. Disposiciones generales sobre el ejercicio de los derechos	196
2.3. Procedimiento para atender el ejercicio de los derechos	199
2.3.1. Ejercicio derecho de acceso de la persona interesada	201
2.3.2. Ejercicio derecho de rectificación	204
2.3.3. Ejercicio derecho de supresión (derecho al olvido).....	205
2.3.4. Ejercicio derecho de oposición.....	211
2.3.5. Ejercicio derecho de portabilidad.....	212
2.3.6. Ejercicio derecho limitación de tratamiento	213
2.4. Aspectos prácticos para atender al ejercicio de derechos.....	214

3. Brechas de seguridad.....	214
3.1. Normativa de aplicación.....	214
3.1.1. Concepto y definición de violación o brecha de seguridad.....	217
3.1.2. Detección de la brecha de seguridad, registro y clasificación.....	219
3.1.3. Obligaciones derivadas de la existencia de una brecha o violación de seguridad para el responsable del tratamiento y para el encargado del tratamiento.....	221
3.1.4. Tipos de las brechas	229
3.1.5. Creación de procedimiento para prevenir una brecha de seguridad	231

CAPÍTULO SEXTO. OBLIGACIONES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO..... 237

1. Análisis de riesgos.....	237
1.1. Normativa de aplicación.....	237
1.2. El análisis de riesgos para identificar medidas de seguridad	238
1.3. Aspectos prácticos en relación con el análisis de riesgos.....	241
2. Evaluación de impacto	242
2.1. Normativa de aplicación.....	242
2.2. ¿En qué consiste una evaluación de impacto? ...	243
2.3. Tabla resumen de una evaluación de impacto ...	260
3. Medidas de protección de datos desde el diseño y por defecto.....	262
3.1. Normativa de aplicación.....	262
3.2. La filosofía de la protección de datos desde el diseño y por defecto.....	263
3.3. Principios que rigen la Protección de datos desde el diseño y por defecto.....	264

3.4. Guías de la Agencia Española de Protección de datos en relación con la protección de datos desde el diseño y por defecto.....	267
3.5. Aplicación práctica.....	272
4. Nombramiento de delegado de protección de datos (DPD).....	274
4.1. Normativa de aplicación.....	274
4.2. Nombramiento de delegado de protección de datos y su comunicación ante la Agencia Española de Protección de datos.....	275
5. ¿Están previstas sanciones para las administraciones Públicas por el incumplimiento de las obligaciones en materia de protección de datos?.....	277
CAPÍTULO SÉPTIMO. LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES EN LAS ENTIDADES LOCALES	
1. Análisis de las bases que legitiman el tratamiento..	283
1.1. Normativa de aplicación.....	283
1.2. Licitud del tratamiento, condiciones para del tratamiento de datos de carácter personal.....	284
1.2.1. El Consentimiento como base legitimadora del tratamiento.....	287
1.2.2. Cumplimiento de una obligación legal, realización de una misión en interés público o ejercicio de poderes conferidos al responsable del tratamiento	290
1.2.3. Interés legítimo.....	293
1.2.4. Datos de características especiales	294
2. Aspectos prácticos de la legitimación del tratamiento	298

2.1. ¿Qué se considera una “obligación legal”?.....	300
2.2. Ejemplos de normas con rango de ley que legitiman el tratamiento.....	300
2.3. Cesión de datos.....	304
2.3.1. Cesión de datos entre Administraciones Públicas.....	304
3. Supuestos Concretos	308
3.1. Ley 39/2015, de 1 de octubre, del Procedimiento administrativo común de las Administraciones Públicas, artículo 28.2 modificado por la LOPDGDD.....	308
3.2. Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.....	314
3.3. Notificaciones en procesos de concurrencia competitiva.....	319
3.3.1. Valoración del consentimiento como una base que legitima el tratamiento en los procesos de selección.....	321
3.3.2. Conflicto entre transparencia y protección de datos.....	322
3.3.3. Conclusiones/recomendaciones.....	323
3.4. Cesión de datos a particulares.....	325
3.5. Acceso a la información por parte de las personas que integran la corporación municipal	329
3.6. Base legitimadora de la interoperabilidad entre las administraciones	338
3.7. La transparencia de las administraciones versus la protección de datos personales.....	340
3.8. Breve referencia a los plazos de conservación de la documentación.....	353
3.9. Reutilización de la información	355
3.10. Salidas de datos de carácter personal.....	360

3.11. Uso de datos biométricos	361
3.11.1. ¿Qué se entiende por datos biométricos?...362	
3.11.2. ¿Será necesario realizar una evaluación de impacto?.....	365
3.12. La videovigilancia por las fuerzas y cuerpos de seguridad del estado	370
3.12.1. Normativa de aplicación.....	370
3.12.2. Consideraciones previas	371
3.12.3. La videovigilancia de espacios públicos ...	374
3.12.4. Comisión de videovigilancia en la Delegación del Gobierno.....	375
3.12.5. Imágenes para el control, regulación, vigilancia y disciplina del tráfico	376
3.12.6. Cámaras móviles	379

CAPÍTULO OCTAVO. MEDIDAS DE SEGURIDAD APLICABLES A LAS ENTIDADES LOCALES SEGÚN EL ESQUEMA NACIONAL DE SEGURIDAD. LA CIBERSEGURIDAD.....381

1. Normativa de aplicación	383
2. Introducción al Esquema Nacional de Seguridad.....	385
2.1. Sujetos obligados	389
2.2. Principios básicos	392
2.3. Objetivos	394
2.4. Plazo de adecuación	395
2.5. Esquema Nacional De Interoperabilidad (ENI) ...	395
3. Fases en la implantación del ENS	396
3.1. Política de seguridad y definición de roles.....	398
3.2. Roles que intervienen	400
3.2.1. Responsable de la información.....	401
3.2.2. Responsable del Servicio	402

3.2.3. Responsable de Seguridad.....	402
3.2.4. Incompatibilidades a la hora de ejercer las funciones entre las figuras establecidas en el ENS	403
3.2.5. Incompatibilidad entre la figura de DPD y Responsable de Sistemas	406
3.3. Identificación de la información del sistema y categorización del sistema.....	407
3.4. Análisis de riesgos	409
3.4.1. Fases del análisis de riesgos	410
3.5. Declaración de aplicabilidad y medidas compensatorias.....	411
3.6. Plan de adecuación y medidas de seguridad.....	412
3.6.1. Marco organizacional.....	414
3.6.2. Marco operacional	415
3.6.3. Medidas de protección.....	422
3.7. Mejora continua	428
4. ENS e ISO 27001	431
5. Centro Criptográfico Nacional promueve la ciberseguridad en las entidades locales.....	432
6. Ciberseguridad.....	436

Bibliografía.....	445
--------------------------	------------