POLÍTICA PLAZOS DE CONSERVACIÓN

1. OBJETO DE LA POLÍTICA

El Reglamento 2016/679, 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 (en adelante, el "RGPD") pretende garantizar y proteger todo lo concerniente al tratamiento de los datos personales, es decir, el uso de cualquier información de personas físicas. Una de las medidas que contempla es la obligatoriedad de los responsables de tratamiento en determinar un plazo de conservación para todos los datos personales que traten en sus respectivas actividades.

Mediante la presente Política de conservación de datos personales, se pretende establecer unas directrices de actuación relativas a determinar cuándo debe procederse a la conservación o a la destrucción de los datos, a los efectos de dar cumplimiento a las exigencias derivadas de los principios del tratamiento contemplados en el artículo 5 del RGPD, en especial el de responsabilidad proactiva.

2. ÁMBITO DE APLICACIÓN

La presente Política deberá ser observada por FUNDACIÓN MANANTIAL, así como por las empresas que traten datos de carácter personal en calidad de Encargados del Tratamiento, cuando FUNDACIÓN MANANTIAL sea Responsable de los mismos. Asimismo, la presente Política es de aplicación respecto de datos que sean objeto tanto de tratamiento automatizado como de tratamiento no automatizado (soporte papel).

La presente Política deberá ser observada por todo el personal que maneje datos de carácter personal en el desarrollo de su actividad diaria.

3. OBLIGACIONES DE SUPRESIÓN DE DATOS PERSONALES

3.1. Consideraciones previas

Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el Responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica.

A tal efecto, la presente Política debe guiarse por Principio de limitación del plazo de conservación del apartado e) del artículo 5.1 del RGPD, en virtud del cual los datos personales deben ser "mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales".

Esta obligación resulta de aplicación para FUNDACIÓN MANANTIAL tanto cuando actúe como Responsable del tratamiento, como cuando lo haga en calidad de encargado del tratamiento.

En particular, cuando la Entidad tenga la consideración de Encargado del Tratamiento, de conformidad con el apartado g) del art. 28.3 del RGPD, una vez cumplida la prestación contractual que dio lugar al encargo del tratamiento, los datos personales deberán, a elección del Responsable, ser suprimidos o devueltos, debiendo suprimir asimismo las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros (regulación sectorial local incluida).

Todo ello sin perjuicio de otras obligaciones que se deriven de lo acordado con el Responsable, relativas a las medidas de seguridad que se deban adoptar o cualquier otra disposición que verse sobre la conservación, bloqueo o destrucción de los datos.

3.2 Causas habilitantes de la supresión de los datos personales

Según el RGPD, la supresión es el procedimiento en virtud del cual el Responsable cesa en el uso de los datos personales, procediendo a su eliminación.

Así, FUNDACIÓN MANANTIAL suprimirá los datos en los siguientes supuestos:

3.2.1 Terminación de la condición legitimadora del tratamiento.

Cuando los mismos ya no sean útiles ni necesarios para la finalidad que justificó su tratamiento. Una vez cumplida y agotada dicha finalidad deberá procederse a la supresión de los datos personales, siempre y cuando no sea necesario proceder al bloqueo de los mismos para

responder ante posibles responsabilidades derivadas del tratamiento de datos personales y por el plazo de prescripción de las mismas previstas en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, conforme se recoge en el apartado 4.

3.2.2 Ejercicio del derecho de supresión

Cuando el interesado ejerza el derecho de supresión de los datos personales, siempre que concurran alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21.1 del RGPD (derecho de oposición), y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento cuando éste tenga por objeto la mercadotécnica directa (artículo 21.2 del RGPD);

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a niños, mencionados en el artículo 8.1 del RGPD.

En estos casos, deberá procederse a la eliminación de los datos personales, siempre y cuando no sea necesario proceder al bloqueo de los mismos para responder ante posibles responsabilidades derivadas del tratamiento de datos personales y por el plazo de prescripción de las mismas.

No obstante lo anterior, no se aplicará el derecho de supresión, y por tanto los datos podrán continuar siendo tratados por el responsable del tratamiento, cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

4. MECANISMOS DE SUPRESIÓN Y BLOQUEO DE LOS DATOS PERSONALES

4.1. Supresión de datos

En los supuestos en que, en atención a los criterios anteriores, se concluya el deber de suprimir los datos personales, se deberá proceder a la eliminación física de los mismos, ya se encuentren éstos en soportes automatizados o no automatizados:

- Si los datos están contenidos en soportes no automatizados, se deberá proceder a la destrucción física de los documentos. A tal efecto se recomienda:
    - La utilización de proveedores de servicio de destrucción documental.
    - La utilización de herramientas de destrucción física de papel, como destructoras de papel.
    - Opcionalmente, y en el caso en que la supresión tenga como origen el ejercicio de derecho de supresión, la supresión podrá tener lugar mediante la entrega de dicha información a la persona o personas que sean titulares de la misma.
    - Si los datos están contenidos en soporte informático, se procederá de igual forma a su eliminación física de la aplicación, sin que sea suficiente el empleo de una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren los derechos de supresión.

Sin perjuicio de cualquier otro método de destrucción que pudiera valorarse, a continuación, se recogen los principales métodos de borrado identificados[1], clasificados en función de la capacidad efectiva para la eliminación lógica de los datos personales, así como sus ventajas e inconvenientes.

Métodos que no destruyen la información de forma segura (comandos de borrado)	Formateo	Formateo de un dispositivo
	Anonimización[2]	Su eficacia dependerá de la técnica de anonimización empleada en cada caso, que deberá garantizar de forma irreversible la imposibilidad de su reidentificación.[3]
Métodos de destrucción de la información de forma segura	Desmagnetización	Exposición de los soportes de almacenamiento a un potente campo magnético.
	Destrucción	Podrá realizarse a través de diversos procedimientos mecánicos, en función de la naturaleza del soporte, en particular: • Desintegración, pulverización, fusión e incineración. • Trituración.
	Sobreescritura	Escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Deberá asegurarse la sobreescritura de la totalidad de la superficie de almacenamiento para asegurar la completa destrucción de los datos.

[1] Fuente. Guía sobre borrado seguro de la información. Instituto Nacional de Ciberseguridad (INCIBE), 2016

[2] El Considerando 26 del RGPD concluye que "Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

[3] Véase "Dictamen 05/2014 sobre técnicas de anonimización" del Grupo de Trabajo del artículo 29.

4.2. Bloqueo de datos personales

FUNDACIÓN MANANTIAL, como Responsable del tratamiento, aplicará técnicas de bloqueo de datos para garantizar la conservación de información personal a efectos de poder atender a posibles reclamaciones.

El bloqueo de los datos consiste en el procedimiento a través del cual el Responsable del tratamiento identifica y reserva datos personales, adoptando medidas técnicas y organizativas para impedir su tratamiento por personas no autorizadas. Estas medidas impedirán su visualización, excepto en lo relativo a la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Cumplidos los indicados plazos, deberá procederse a la supresión de los datos bloqueados de acuerdo con lo descrito en la tabla anterior.

Sin perjuicio de cualquier otro método de bloqueo que pudiera valorarse, a continuación, se recogen las principales técnicas de bloqueo identificadas:

Métodos para aplicar bloqueo físico de la información personal	Clasificación confidencial	Podrá crearse una ubicación/armario confidencial.
	Acceso restringido y cambio de ubicación	Limitar el acceso a la información bloqueada guardándola en el armario o ubicación confidencial.
Métodos para realizar el bloqueo automatizado de la información personal	Descarga de información del correo electrónico en correos locales fuera del servidor de correo. Acceso restringido a archivos	Descarga de los archivos a una carpeta en red de uso privado del usuario + Contraseña de acceso a la carpeta.
	Invisibilizar elementos a través de gestión de	Dependerá de las capacidades técnicas del sistema o las

	permisos y privilegios o configuración de carpetas/archivos	opciones de configuración del software utilizado.
	Protección de archivos con contraseñas de acceso o protección	Para impedir el tratamiento de datos bloqueados podrá establecerse contraseñas que eviten la consulta, utilización, destrucción.
	Establecimiento de regla de correo electrónico para el borrado automatizado de información	Permite llevar a cabo la aplicación de la política de conservación de datos (bloqueo y supresión) de forma automática.

Importante: Si la configuración del sistema no permite el bloqueo o supone un esfuerzo excesivo, se puede realizar un copiado seguro de la información, que acredite la autenticidad, la fecha del bloqueo y la no manipulación de los datos durante el bloqueo.

5. PLAZOS DE CONSERVACIÓN DE DATOS SEGÚN ACTIVIDADES DE TRATAMIENTO

Área	Documento	Plazo de Conservación
Fiscal y contable	A efectos mercantiles Libros, correspondencia, documentación y justificantes concernientes al negocio, debidamente ordenados, a partir del último asiento realizado en los libros, salvo lo que se establezca por disposiciones generales o especiales. Esta obligación mercantil se extiende tanto a los libros obligatorios (ingresos, gastos, bienes de inversión y provisiones, además de la documentación y	6 años

	justificantes en que se soporten las anotaciones registradas en los libros (facturas emitidas y recibidas, tickets, facturas rectificativas, documentos bancarios, etc.).	
	Cuentas anuales, los contratos a largo plazo, las copias de seguridad de los registros contables o las acciones adquiridas por la empresa (en previsión de una futura venta).	Indefinidamente
	<u>A efectos fiscales</u> Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc.), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tenga trascendencia fiscal).	4 años
Laboral, PB&D, Empleo y Transformación Social	Nóminas, contratos de trabajo y cualquier documentación relacionada con la actividad laboral y la Seguridad Social	4 años desde la finalización de la relación laboral con el empleado.
	Currículums	Hasta el fin del proceso de selección, y 1 año más con consentimiento del interesado.
	Buzón del Canal Ético	Anonimización de los datos transcurridos seis meses (como máximo) desde la finalización de la clarificación de los hechos,

		salvo que sean investigados en un entorno legal distinto.
Comunicación	BBDD, web, redes sociales, boletines, newsletters, etc.	Indefinidamente, hasta la revocación del consentimiento o el ejercicio de derechos.
Subvenciones y AAPP	Toda la documentación relativa a esta área	Durante el plazo que determine la normativa específica de cada convocatoria. Además, es recomendable conservar esta documentación durante al menos 4 años desde el momento de la justificación de la subvención o ayuda.
RAS	Historias clínicas como Responsable del Tratamiento	Mínimo 5 años desde la salida.
SIC y Calidad	Auditorías	5 años
General	Documentación almacenada como Encargados del Tratamiento	Durante los plazos determinados por el Responsable del Tratamiento

TIPO DE DOCUMENTO		PLAZO	BASE LEGAL
Documentación sujeta a la normativa de PBCFT	Documentación en que se formalice el cumplimiento de las obligaciones establecidas en la Ley (información fiscal y contable,	10 años	Artículo 25. Ley 10/2010 de prevención del blanqueo de capitales y de la financiación del terrorismo.

	donaciones, documentos de identidad).		Los sujetos obligados conservarán durante un período de diez años la documentación en que se formalice el cumplimiento de las obligaciones establecidas en la presente ley.