PROTOCOLO DE ACTUALIZACIÓN Y CONSERVACIÓN DE DATOS

1. Principios

El artículo 5 del Reglamento (UE) 2016/679, de 27 de abril (GDPR), relativo a los principios del tratamiento, dispone:

Artículo 5.1.d): *los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»)*.

Artículo 5.1.e): *los datos personales serán 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; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»)*.

Por lo que la Organización ha establecido un protocolo de actuación para cumplir dichos principios destinado a implementar procedimientos que permitan la exactitud y la limitación del plazo de conservación de los datos personales tratados bajo su responsabilidad, protocolo que tiene en cuenta los siguientes criterios para:

- La actualización de los datos.
- La conservación de los datos.
- Los datos en régimen de custodia.
- El bloqueo de datos.
- La eliminación y/o destrucción de datos.

Además, la Organización ha implementado las siguientes medidas para demostrar el cumplimiento de este protocolo de actuación:

- Medidas técnicas y organizativas de seguridad desde el diseño y por defecto.
- Repositorio de evidencias (accountability).

Los responsables del tratamiento, o sus representantes, deberán poner a disposición del responsable de privacidad de la Organización este protocolo para su aplicación en todas las fases del tratamiento.

2. Criterios para la actualización de los datos

Los criterios de actualización de datos se basarán en el derecho de rectificación de los datos (art. 16 y 19 GDPR), por el cual el interesado tiene derecho a que el responsable rectifique sus datos sin demora injustificada cuando resulten inexactos o incompletos con respecto a los fines para los que se tratan, mediante una declaración rectificativa adicional.

El responsable podrá solicitar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de rectificación.

En el caso de fallecidos, este derecho lo podrán ejercitar las personas vinculadas al mismo por razones familiares o de hecho, así como sus herederos o las que hubiere designado expresamente para ello, excepto si el causante lo hubiese prohibido expresamente o así lo establezca una ley.

La Organización deberá poner a disposición del interesado las herramientas adecuadas para actualizar los datos cuando se prevea que puedan ser inexactos o incompletos mediante:

- Procedimientos para facilitar al interesado la modificación de sus datos.
- Procedimientos para comunicar las modificaciones a los destinatarios de los datos.
- Procedimientos para que el responsable pueda actualizar los datos periódicamente.
- Procedimientos para que el interesado pueda actualizar directamente sus datos por internet.

Para aplicar los criterios de actualización se deberán tener en cuenta, entre otras, las siguientes operaciones de tratamiento:

- La obtención de datos:
  - Datos facilitados directamente por el interesado.
  - Datos facilitados por terceros mediante la comunicación o transmisión de datos.
  - Datos disponibles por el responsable porque los ha tratado previamente.
  - Datos capturados de forma autónoma por dispositivos o aplicaciones.
- El registro de datos:
  - Formularios electrónicos dispuestos en una aplicación local.
  - Formularios electrónicos dispuestos en una aplicación por internet.
  - Formularios en papel para su posterior registro electrónico.
  - Comunicación mediante correo electrónico.
  - Comunicación mediante correo postal.
  - Comunicación mediante llamada telefónica.
  - Fichas de datos en papel (tratamiento no automatizado).
- La conservación de datos:
  - Datos conservados en sistemas simples de ficheros.
  - Datos conservados en bases de datos estructuradas.
  - Datos conservados en bases de datos documentales.
  - Datos ubicados en dispositivos locales propios.
  - Datos ubicados en dispositivos externos propios (nube).
  - Datos ubicados en dispositivos externos ajenos (nube).
  - Procedimientos para realizar copias de seguridad periódicamente.
- El acceso a datos
  - Permisos para el acceso a datos (crear, consultar, modificar y eliminar).
  - Permisos para usar la información (visualizar, copiar, imprimir, listar, agrupar, filtrar, calcular, analizar, enviar, exportar, etc.).

3. Criterios de conservación de los datos

Los criterios de conservación de los datos se basarán en mantenerlos durante no más tiempo del necesario para alcanzar el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia y cuando ya no sea necesario para ello, se suprimirán con medidas de seguridad adecuadas para garantizar la anonimización de los datos o la destrucción total de los mismos.

La Organización facilitará las herramientas adecuadas para suprimir los datos cuando los criterios de conservación así lo determinen, mediante:

- Procedimientos para facilitar al interesado el derecho de supresión de sus datos.
- Procedimientos para comunicar las supresiones a los destinatarios de los datos.
- Procedimientos para que el responsable pueda suprimir los datos o anonimizarlos.
- Procedimientos para que el interesado pueda suprimir directamente sus datos por internet.

Se podrán conservar los datos durante períodos más largos siempre que se traten exclusivamente con:

- Fines de archivo en interés público.
- Fines de investigación histórica, estadística o científica

El derecho de supresión de los datos (art. 17 y 19 GDPR), por el cual el interesado tiene derecho a que el responsable deje de mantener sus datos y los suprima sin demora injustificada, se podrá ejercer siempre que:

- El tratamiento sea ilícito.
- El interesado haya retirado su consentimiento, cuando el tratamiento se base en este.
- Los datos ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados.
- Los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información (e-commerce).
- El interesado haya ejercido el derecho de oposición y no prevalezcan otros motivos legítimos para el tratamiento.
- Los datos deban suprimirse para cumplir una obligación jurídica del responsable.

Cuando la supresión derive del ejercicio del derecho de oposición, el responsable podrá conservar los datos identificativos del interesado con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

En el caso de fallecidos, este derecho lo podrán ejercitar las personas vinculadas al mismo por razones familiares o de hecho, así como sus herederos o las que hubiere designado expresamente para ello, excepto si el causante lo hubiese prohibido expresamente o así lo establezca una ley.

No se dará curso al derecho de supresión de datos cuando:

- Prevalezca el derecho a la libertad de expresión e información.
- Exista una obligación jurídica del responsable que le obligue a conservarlos.
- Sea necesario para la formulación, ejercicio o defensa de reclamaciones.
- Exista un interés público fundamentado en la legislación vigente por razones de salud pública o para fines de investigación histórica, estadística o científica.

4. Datos en régimen de custodia

Una vez finalice el plazo de conservación previsto, no procederá la supresión de datos cuando se requiera su conservación por una previsión legal, en cuyo caso la Organización procederá a la custodia de los mismos bloqueando los datos y limitando su tratamiento en tanto que pudieran derivarse responsabilidades de su relación con los intervinientes en el tratamiento o con los interesados afectados por el mismo.

Los datos podrán conservarse durante períodos más largos de los establecidos, siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Para estos casos, se deberán aplicar las medidas técnicas y organizativas que dispone el artículo 89.1 GDPR a fin de proteger los derechos y libertades del interesado.

Los datos deberán conservarse con especial amparo de manera que se puedan ejercer los derechos del interesado establecidos en los artículos 15 al 22 del GDPR, especialmente cuando se prevea el bloqueo de los datos o la limitación u oposición al tratamiento. Para su puesta en práctica, se seguirá el Protocolo para el ejercicio de los derechos del interesado que la Organización pone a disposición del personal autorizado para el tratamiento de datos.

Los derechos del interesado que afectan especialmente a la conservación de los datos son:

- Derecho de supresión de los datos (derecho al olvido) (art. 17 GDPR)
- Derecho a la limitación del tratamiento (art. 18 GDPR)
- Derecho de oposición al tratamiento (art. 21 GDPR)

5. Bloqueo de datos

De conformidad con el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), el responsable del tratamiento está obligado a bloquear los datos cuando proceda a su rectificación o supresión hasta finalizar el plazo de prescripción de sus responsabilidades. Transcurrido dicho

plazo, deberá proceder a su destrucción.

El bloqueo de datos consiste en la identificación y reserva de los datos para la exigencia de posibles responsabilidades derivadas del tratamiento, adoptando medidas técnicas y organizativas para impedir su tratamiento, incluida su visualización. Los datos bloqueados no podrán ser tratados para ninguna otra finalidad.

Solo se podrá acceder a estos datos para exigir responsabilidades y solo durante el tiempo de prescripción para la conservación de los mismos. En este sentido, se deberá disponer en los sistemas de información de un campo para señalar el tiempo de conservación y funcionalidades específicas para suprimir dichos datos cuando haya concluido su prescripción.

Este tratamiento obliga a configurar los sistemas de información (siempre que sea posible) para poder tener una copia de los datos originales antes de ser modificados o suprimidos. Si los sistemas de información no permiten realizar esta copia, se deberán escanear dichos datos antes de su modificación o supresión y custodiarlos de manera que no se tenga acceso a ellos.

Alternativa a la obligación del bloqueo de datos, cuando la configuración del sistema de información no permita el bloqueo o requiera una adaptación que implique un esfuerzo desproporcionado:

- Se procederá a una copia segura de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

6. Eliminación y/o destrucción de datos

Cualquier documento físico o soporte digital que quiera ser eliminado y que incluya datos personales, debe ser destruido con la destructora o retirado por una empresa homologada de destrucción de documentos.

El personal deberá almacenar toda la información tratada en el directorio de red correspondiente indicado por el responsable de privacidad, lo que permitirá que a esta información se le apliquen las medidas de seguridad existentes y que se sometan los procedimientos de copias de seguridad aplicados por la organización.

Los procedimientos para la eliminación y/o destrucción de datos que empleará la Organización son:

- Datos conservados en formato digital:
    - Eliminación semanal de los documentos contenidos en la Papelera.
    - Revisión semanal de los archivos contenidos en carpetas temporales y Escritorio.
    - Eliminación mensual de las copias de seguridad antiguas.
- Datos conservados en formato físico:
    - Recolección inmediata de documentación expedida por las impresoras comunes.
    - Destrucción de documentos mediante destructora de papel.
    - Destrucción de soportes que contengan datos con medidas de seguridad.

7. Medidas técnicas y organizativas de seguridad.

Confidencialidad de la información

- Procedimientos con datos automatizados (digital)
    - Acceso durante el tratamiento digital (pantallas):
        - se tratarán impidiendo la visión de los datos a personas no autorizadas.
    - Almacenamiento de los soportes digitales:
        - se guardarán en un mobiliario y/o departamento con medidas de seguridad o en locales externos autorizados por el responsable.
    - Destrucción de soportes digitales:

        - se utilizarán destructoras de soportes digitales o empresas homologadas con certificación de destrucción.

- Procedimientos con datos no automatizados (manual)
    - Acceso durante el tratamiento manual (documentos):
        - se tratarán impidiendo el acceso a los datos a personas no autorizadas.
    - Almacenamiento de documentos:
        - se guardarán en un mobiliario y/o departamento con medidas de seguridad o en locales externos autorizados por el responsable.
    - Destrucción de documentos:
        - se utilizarán destructoras de papel o empresas homologadas con certificación de destrucción.

Integridad de la información

- Copias de respaldo:
    - Ubicación de las copias:
        - se guardarán en un mobiliario y/o departamento con medidas de seguridad y en un hardware distinto del que las crea (copia interna o de red).
    - Periodicidad de programación:
        - se realizará semanalmente, como mínimo.
    - Periodicidad de comprobación de datos:
        - se realizará, como máximo, a los 6 meses desde la creación de la copia.
    - Método de comprobación de datos:
        - se realizará preferiblemente mediante una aplicación informática de verificación de copias, aunque también se podrá hacer manualmente.

- Copias de respaldo externas:
    - Ubicación de las copias externas:
        - se guardarán en un local y/o departamento distinto de donde se creó con medidas de seguridad o en servicios de backup de Internet.
    - Periodicidad de programación de las copias externas:
        - se realizará semanalmente, como mínimo.
    - Cifrado de los datos de las copias externas:
        - se cifrarán cuando las copias salgan de los locales de la empresa.

- Disponibilidad de los datos:
    - Actualización de software:
        - se actualizarán periódicamente los sistemas operativos y las aplicaciones informáticas con las últimas versiones disponibles.
    - Sistemas de detección de intrusos y prevención de fuga de información:
        - se implementarán sistemas de protección tipo firewall, antivirus, antispam, antiphishing, antimalware, antiransomware, etc.
    - Disponibilidad de los servicios de información:
        - se implementarán medidas adecuadas para garantizar la disponibilidad de los datos.
    - Restauración de los servicios de información:
        - se implementarán medidas adecuadas para restaurar rápidamente la disponibilidad y el acceso a los datos.
    - Resiliencia de los servicios de información:
        - se implementarán medidas adecuadas para anticiparse y adaptarse a cambios imprevistos en los servicios de información.
    - Procesos de verificación, evaluación y valoración de las medidas de seguridad:
        - se implementarán procesos para verificar, evaluar y valorar la eficacia de las medidas de seguridad implementadas.

8. Repositorio de evidencias (accountability)

El repositorio de evidencias contendrá la documentación considerada relevante a la hora de demostrar la responsabilidad proactiva de la Organización (accountability).

El responsable de privacidad se encargará de cumplir y hacer cumplir este Protocolo de actualización y conservación de datos y de establecer los procedimientos adecuados para registrar las evidencias, como son:

- Sistema de aviso del vencimiento del plazo para actualizar datos.
- Sistema de aviso del vencimiento del plazo de conservación de datos.
- Sistema para el registro de datos dispuestos en régimen de custodia.
- Sistema para el registro de datos bloqueados.
- Sistema de comprobación de los procesos de eliminación y/o destrucción de datos.
- Sistema de verificación de las medidas técnicas y organizativas de seguridad.
- Auditoría periódica de los procesos para la actualización y mejora de los mismos.