Universidad de Buenos Aires
Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería
Maestría en Seguridad Informática

Plan de Tesis de Maestría

Título:

Análisis de la Política de Protección General de Datos en Europa (GDPR – General Data Protection Regulation)

Consecuencias, Compatibilidad, implementación y casos particulares de GDPR

Autor: Pablo Cababie

Director/a de Tesis: Lic. Graciela Pataro

Año de Presentación: 2017

Cohorte del Maestrando: 2009

Declaración jurada de contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Buenos Aires, Octubre de 2017.-

FIRMADO: Pablo Cababie

Índice de contenidos 3

RESUMEN

El presente trabajo de tesis abarcará un intensivo análisis de la política GDPR [2] próxima a implementarse en Europa en 2018.

A consecuencia de estas medidas, las empresas se ven obligadas a adaptarse a las diferentes políticas en los distintos países en los que operan. En muchos casos hay similitudes y en otros las diferentes perspectivas, condiciones y cultura hacen que la política de privacidad sea diferente. Por ello, a lo largo del desarrollo del trabajo se contemplará la compatibilidad con políticas similares de otros países y regiones.

Principalmente se ha elegido efectuar un análisis comparativo con las políticas implementadas y vigentes en EEUU y Canadá (PIPEDA), los cuales presentan antecedentes implementando este tipo de políticas y son pioneros en la materia.

El desarrollo a su vez cubrirá aspectos clave de la política GDPR como la creación de un inventario de datos, necesidad, retención y eliminación de la información, integridad y calidad de la data almacenada, nuevos procesos para transferencia de datos, procedimientos ante filtración de información y consentimiento de recolección y almacenamiento de datos, entre otros.

Asimismo, se espera efectuar un análisis extensivo de las consecuencias de la implementación de la ley. Esta nueva política exige la necesidad de capacitación y creación de puestos de trabajo mediante el rol de “Data Protection Officer”, quien debe reportar directo a la alta dirección de la compañía para poder informar y operar con independencia.

Si bien está implícito en todo cambio organizacional, el factor económico es un componente importante a tener en cuenta en estas situaciones, por lo que se procederá a efectuar un análisis de costos hipotético y orientativo de implementación para poder estar alineado con la nueva ley.

También, se investigará en profundidad particularmente como la nueva ley contempla los casos de computación en la nube y Big Data dado su exponencial crecimiento y continuo avance.

Por último se propondrá un método para medir la efectividad y alineamiento de la corporación con esta ley que pueda ser utilizado por auditores o implementadores como guía básica.

Palabras clave
GDPR, Privacidad, Política, Regulación, Datos, Información, Europa

Nómina de abreviaturas

- ET: Encargado del tratamiento de los datos
- RT: Responsable del tratamiento de los datos
- DPO: Delegado de Protección de Datos
- FTC: “Federal Trade Commission”: Cámara Federal de comercio
- PIPEDA: “Personal Information Protections and Electronic Documents Act”: Ley de protección de información personal y documentos electrónicos
- ERP: “Enterprise Resource Planning": sistemas de Planeamiento de Recursos Empresariales.
- CRM: “Customer Relationship Management”: sistemas de Gestión de relaciones con los clientes
- UE: Union Europea

Glosario

Seudonimización:
el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable [36]
Los datos seudonimizados se utilizan para ocultar identidades por ejemplo en los ámbitos estadístico e investigador y, normalmente, suele quedar un rastro entre el seudónimo y la identidad con la que corresponde, de manera que permiten singularizar a los interesados y vincularlos entre conjuntos de datos diferentes. Por ejemplo, los datos cifrados a los que se asignan una clave para descifrarlos. Este tipo de datos entra dentro del ámbito de aplicación del régimen jurídico de la protección de datos.
Minimización: Los datos procesados deben limitarse a lo estrictamente necesario e indispensable para el objetivo concreto. El acceso solo debe otorgarse a aquellas personas que los necesiten para dicho fin particular.
Nube hibrida:
Una nube híbrida es un entorno informático que combina una nube pública y una nube privada, y permite que se compartan datos y aplicaciones entre ellas. Cuando la demanda de recursos informáticos y procesamiento fluctúa, la informática en nube híbrida permite a las empresas escalar sin problemas su infraestructura local en la nube pública para poder administrar cualquier flujo de trabajo, sin necesidad de permitir que centros de datos de terceros accedan a todos sus datos. Las organizaciones obtienen la flexibilidad y la capacidad informática de la nube pública para tareas informáticas básicas y menos delicadas, mientras que mantienen las aplicaciones y los datos críticos para la empresa en la infraestructura local, a salvo detrás de un firewall de la compañía.[37]

1. Características generales de GDPR

1.1. Antecedentes

El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), de 4 de noviembre de 1950, consagra el derecho al respeto de la *vida privada y familiar: «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia».[6]*

La Comunidad Europea se crea en 1978 con el Tratado de Funcionamiento de la Unión Europea bajo la necesidad de la integración continental, incorporando la cooperación intergubernamental y reforzando las instituciones comunitarias. La iniciativa la tomó el Parlamento Europeo en 1990 en la Cámara de Estrasburgo aprobando "la Unión Política, sobre una base federal, junto al mercado único y la Unión Económica y Monetaria".

En definitiva, nace la federación de estados, la Unión Europea.

El tratado se apoya en 3 pilares, el comunitario, el de política exterior y seguridad común y el de cooperación policial y judicial en materia penal.

Como consecuencia de la antigua estructura de pilares, actualmente están en vigor diferentes instrumentos legislativos, entre los que figuran instrumentos pertenecientes al antiguo primer pilar, como

- la Directiva 95/46/CE relativa a la protección de datos,
- la Directiva 2002/58/CE (modificada en 2009) sobre la privacidad y las comunicaciones electrónicas,
- la Directiva 2006/24/CE sobre la conservación de datos (declarada inválida por el Tribunal de Justicia de la Unión Europea el 8 de abril de 2014 al constituir una injerencia de especial gravedad en la vida privada y la protección de datos) y
- el Reglamento (CE) 45/2001 relativo al tratamiento de datos personales por las instituciones y los organismos comunitarios,
- así como instrumentos pertenecientes al antiguo tercer pilar relativos a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. [6]

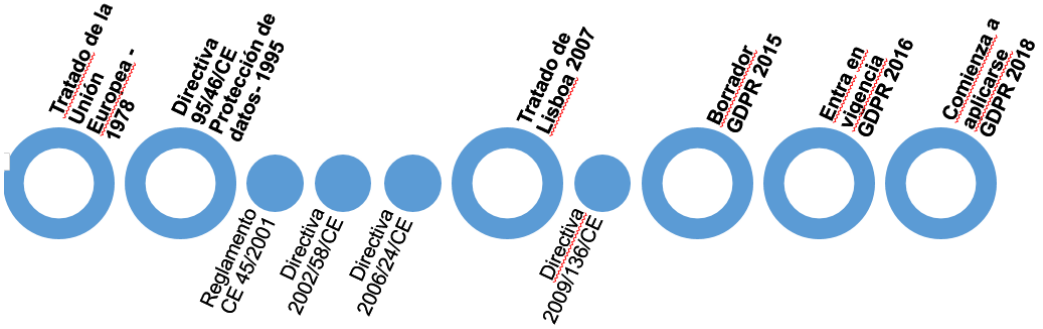


Figura 1 - Cronología de antecedentes a GDPR

La directiva vigente de privacidad de datos personales 95/46/EC [7] fue implementada el 24 de Octubre de 1995. La misma tiene como objetivo la armonización de las leyes relativas al tratamiento y transferencia de datos personales aun fuera de la unión europea. Esta reglamentación representa el primer eslabón de la cadena para la conformación de GDPR. En ella se inscribe la creación de una autoridad pública independiente denominada Autoridades de Protección de Datos (DPA) en cada Estado miembro para supervisar la aplicación de las normas y actuar como organismo para la regulación de las interacciones con empresas y ciudadanos.

A su vez, la directiva prevé la posibilidad de transferir datos personales a terceros países, a condición de que dichos países dispongan de los niveles adecuados de protección de los datos que se garantizarían ser comparables a las protecciones en la Unión Europea. [1]

En general, la directiva se mantiene fiel a los conceptos básicos de privacidad como un derecho humano fundamental. Como es de esperarse, la misma no pierde vigencia hasta la implementación total de la nueva reglamentación en análisis

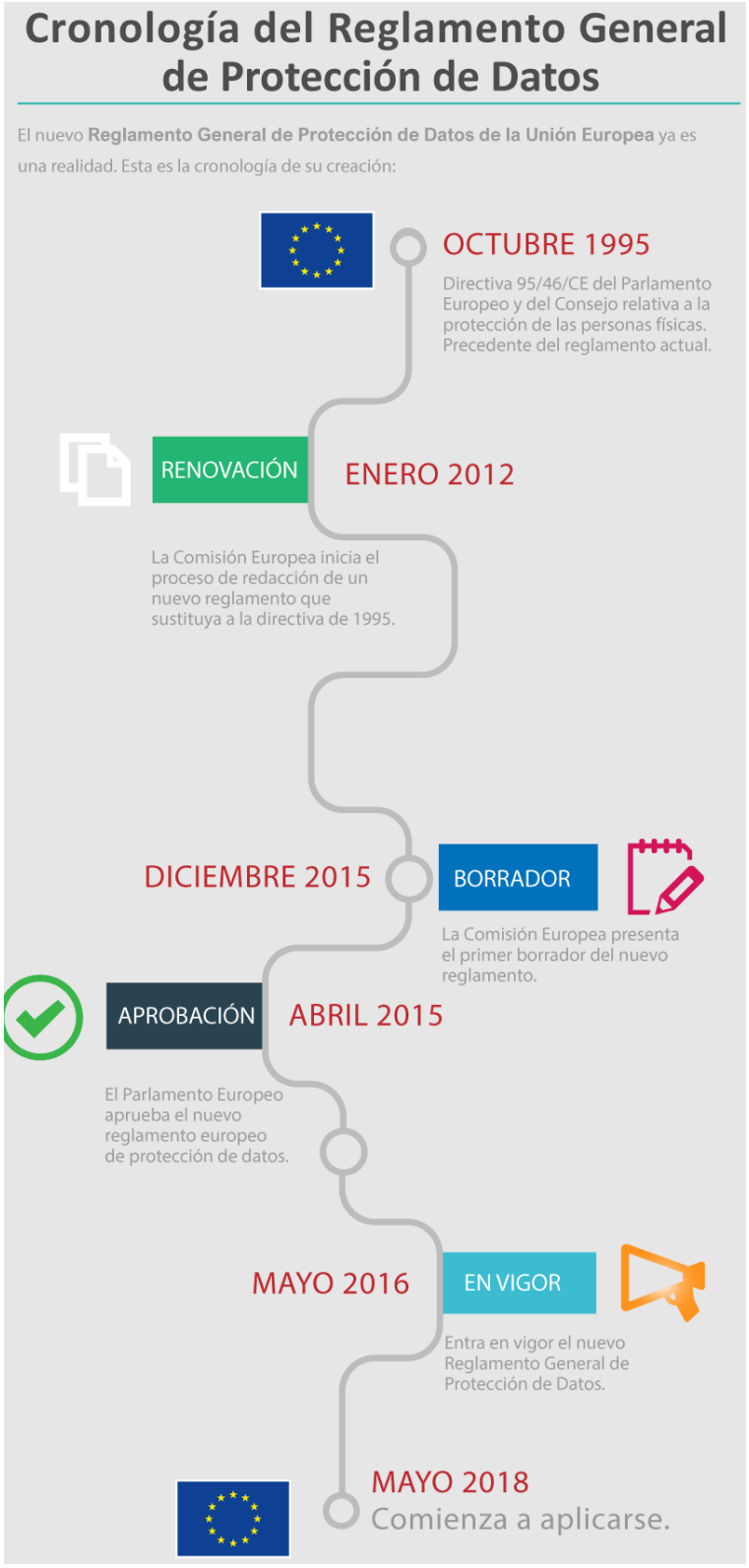


Figura 2- Cronología de la reglamentación GDPR [5]

1.1.1. Diferencias entre Directiva y Regulación

Una Directiva se focaliza en el resultado que debe ser logrado. En este caso, cada miembro de la Unión Europea puede utilizar cualquier forma o metodología que desee para conseguir el resultado requerido

Una Regulación, en cambio, es más abarcativa y se centra en todo el proceso: desde la metodología utilizada hasta el resultado.

Es decir que una Regulación es un conjunto de leyes que obligan a las organizaciones que operen con datos personales (en este caso de individuos de la unión europea), a alinearse y adecuar sus procesos para manejar la información personal como se encuentra legislado.

1.2. Características de la política

El Diario Oficial de la UE ha publicado el Reglamento Europeo de Protección de Datos el día 4 de mayo de 2016, entrará en vigencia a partir del 25 de mayo próximo y es de aplicación obligatoria en cada Estado miembro de la UE a partir del 25 de mayo de 2018.

El 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 deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).[7]

Si bien este reglamento se basa en algunos de los principios básicos del régimen actual de la Unión Europea, los muchos conceptos nuevos que introduce van a requerir una orientación clara y, a menudo, importantes reformas operacionales.

Se espera que este sea el caso con las reglas mucho más estrictas en torno a la obtención del consentimiento de los individuos, las notificaciones de brechas de seguridad, las evaluaciones obligatorias del impacto sobre la privacidad, o el requerimiento de “privacidad por defecto y desde el diseño”, que deberá ser alcanzado gracias a un procesamiento transparente y al cifrado de la información personal.

Además de impactar en las empresas, el reglamento efectuará un cambio en la vida de los individuos, dándoles un mayor control y derechos sobre su información personal. Como resultado, los individuos podrán solicitar que las empresas borren sus datos personales que ya no sean necesarios o correctos, usando el derecho al olvido.[9]

En general esta nueva política prevé que toda comunicación sea clara, precisa y con un lenguaje comprensible sobre las cláusulas de privacidad (sin letras chicas)

En definitiva, la nueva normativa define nuevos y más exigentes requisitos sobre el procesamiento, almacenamiento, transferencia y destrucción de los datos personales.

La normativa establece que las empresas deben disminuir al mínimo la información recolectada y la retención de los datos (el tiempo que se mantienen los datos)

1.2.1. Definición de datos personales

La nueva normativa, define datos personales como cualquier información relacionada a una persona física identificada o identificable. El término “Identificable” hace referencia a que la persona puede ser identificada directa o indirectamente, ya sea a través de un número de identificación o distintos factores de identificación física o social.

1.2.2. Alcance

La normativa impacta organizaciones que administren, procesen, almacenen o recolecten datos personales de individuos que pertenezcan a la Unión Europea.

En particular afecta a:

- Organizaciones que se encuentran físicamente en la Unión Europea o que almacenan sus datos físicamente allí, independientemente de si procesan o no los datos allí.
- Organizaciones que no se encuentran físicamente dentro del territorio de la Unión europea pero ofrecen bienes o servicios dentro de la misma o a individuos que pertenezcan a ella.

1.2.3. Tratamiento de los datos

La reglamentación define la actividad de tratamiento de los datos como:

- Identificar y estructurar los datos personales en archivos según su finalidad.
- Categorizar cada archivo de acuerdo a su tipo de dato (Básicos, Especiales o Penales).
- Asociar cada archivo a un responsable o encargado de tratamiento

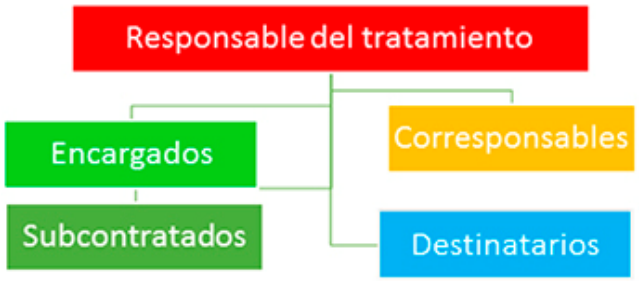
- Identificar si algún archivo pertenece a alguna de las categorías especiales (Alto riesgo, Transferencias internacionales, Elaboración de perfiles, etc.).

Adicionalmente la ley establece categorías de datos y de tratamiento:

Categorías de datos	Básicos
	Especiales
	Penales
Categorías de tratamiento	Tratamiento con alto riesgo Transferencias internacionales de datos Elaboración de perfiles
	Datos tratados por grupos de empresas Datos de titularidad o interés público

Tabla 1. Categorías de Datos y de tratamiento de GDPR

Del mismo modo, la norma, contempla la siguiente designación de responsabilidades para el tratamiento de los datos:



[15]

Ver Figura 11 - Anexo

La siguiente figura ilustra sintéticamente los diferentes actores en el tratamiento de la información y sus funciones

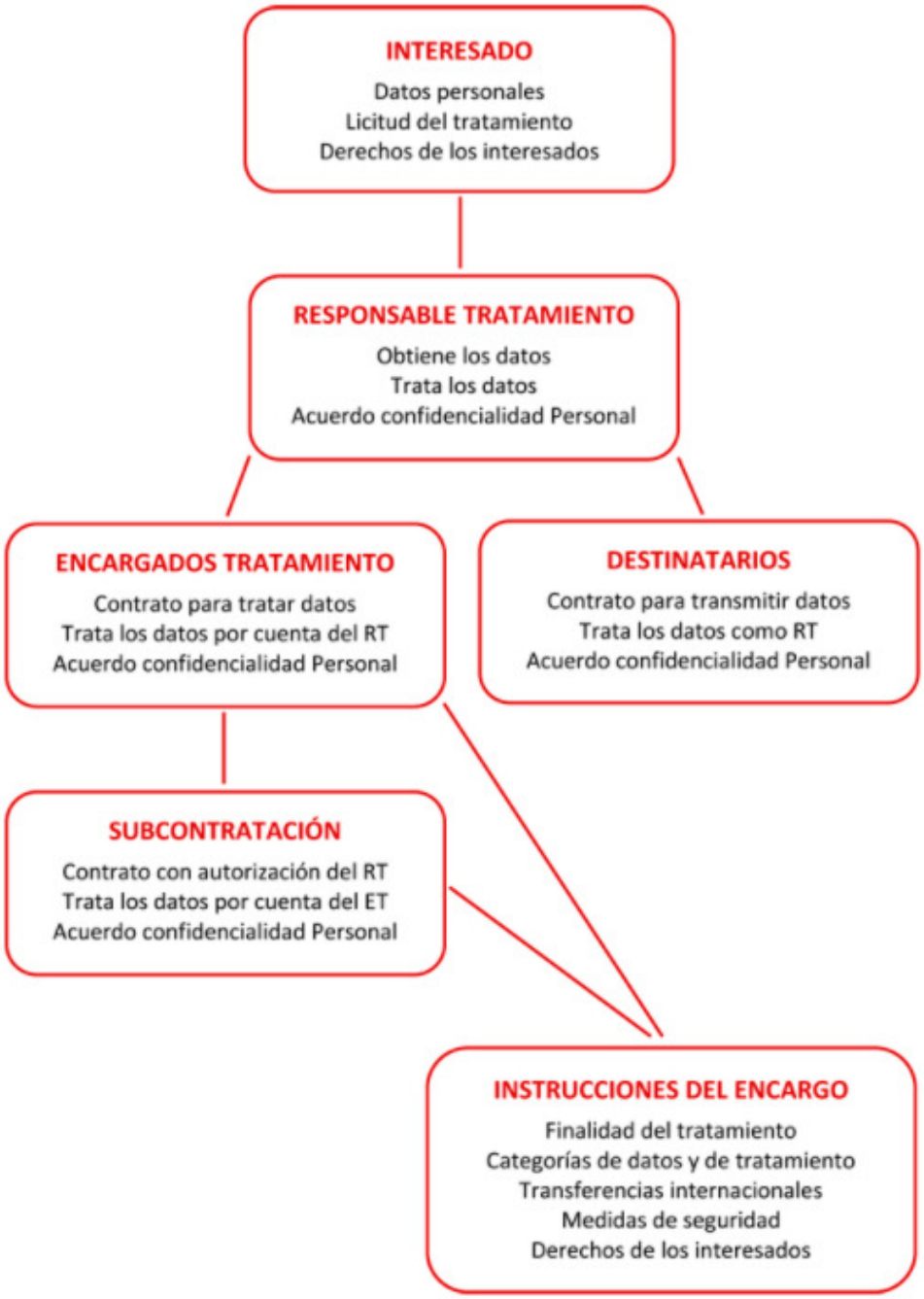


Figura 3- Tratamiento de los datos [15]

1.2.4. Consentimiento claro, afirmativo y activo

La reglamentación establece reglas más específicas y claras con respecto al consentimiento de la persona de la cual se utiliza información.

A partir de ahora para brindar un consentimiento de uso de datos privados ya no bastará con que las empresas le den la opción al usuario de evitar el uso de sus datos personales con simplemente destildar una casilla. Por el contrario, el silencio, inactividad y las casillas pre-chequeadas no representarán un permiso para el uso de los datos recolectados.
También, con esta nueva normativa se requerirá un consentimiento verificable, con lo cual el responsable del tratamiento debe ser capaz de demostrar el consentimiento del usuario.

1.2.4.1. Requisitos de un consentimiento válido:

- Información específica: El texto debe ser preciso y evitar ambigüedades o términos genéricos. Se debe explicitar el propósito exacto y finalidad de la recolección de la información.
- Temporalidad: El consentimiento debe brindarse antes del comienzo del tratamiento.
- Elección activa: El consentimiento debe ser inequívoco y debe ser una voluntad explícita del interesado sin duda alguna respecto a su intención.
- Libremente brindado: El consentimiento será válido solo si el usuario está en condiciones de ejercer una elección real, sin riesgo de engaño, intimidación, coacción y/ o consecuencias negativas en caso de que el mismo no sea brindado.

1.2.4.2. Condiciones del consentimiento:

- Quien vaya a almacenar o tratar los datos deberá probar el consentimiento. Si el mismo es escrito, deberá encontrarse separado de otros temas.
- No puede estar condicionado a la prestación de un servicio sin ser necesario para su realización.
- El usuario deberá ser correctamente notificado acerca de su derecho a revocar el mismo en cualquier momento.

- El responsable deberá brindar un método de revocación de permiso de igual facilidad de acceso que el de brindarlo. Es decir que debería ser igual de simple y fácil, brindar acceso que revocarlo.
- Los consentimiento que no cumplan en su totalidad todas las condicionas serán considerados nulos.

1.2.5. Portabilidad

La nueva reglamentación dispone la facilidad de traspasar datos personales de un servicio a otro, por lo que cambiar de proveedor de correo sin perder emails y contactos en forma transparente será posible. Con esta disposición se logrará brindar al usuario un mayor control de su información y a su vez estimular la competitividad en el mercado digital.

1.2.6. Notificaciones

El robo de datos personales hoy en día es un tema que preocupa al ciudadano digital. Constantemente escuchamos en las noticias de intrusiones, robo de información y filtraciones. Casos como Snowden, Panamá papers son los casos más emblemáticos, pero sin embargo sabemos que existen más de las cuales el usuario nunca se entera. Por ello, la normativa insta a las empresas a informar a las autoridades correspondientes lo más rápido posible sobre cualquier filtración de información o problema de seguridad identificado de modo que los usuarios puedan tomar las medidas necesarias para minimizar el impacto del problema.

En particular la norma exige a las organizaciones a notificar cualquier violación de la seguridad de los datos almacenados a la Autoridad de Protección de Datos dentro de las 72 hs. posteriores a identificar la violación. Es obligatoria la notificación a todos los individuos afectados.

1.2.7. Elaboración de perfiles

Una técnica muy utilizada para el análisis de datos en la cual se usan intensivamente nuestros datos personales consiste en el “profilling”.

Mediante esta metodología se pretende predecir el comportamiento, rendimiento o preferencia agrupando el perfil de cada individuo con perfiles similares.

Si bien esta técnica implica de algún modo la anonimización de los datos (al agrupar perfiles, se perdería la identidad del individuo), la misma será autorizada siempre y cuando exista consentimiento explícito de la persona involucrada. Cabe destacar que durante el tratamiento de los datos y procesos de "profilling" no se podrá discriminar en base a información sensible como origen étnico, posturas políticas, religión o problemas judiciales anteriores.

Para asegurar que todo esto ocurra, la ley exige que el proceso no pueda ser totalmente automático requiriendo supervisión humana continua.

1.2.8. Protección especial para menores de edad

La ley estipula una protección especial para los menores, ya que ellos son menos conscientes de sus actos, los riesgos implícitos y las consecuencias de revelar información privada.

Bajo este inciso se encuentra, por ejemplo la necesidad de un permiso paternal para que un menor abra una cuenta en una red social.

Queda a criterio de cada autoridad la definición de los rangos de edad a los cuales aplica esta protección especial, pero debe situarse entre los 13 y 16 años.

1.2.9. Privacidad por defecto desde el diseño

La Privacidad desde el diseño consiste en la implantación de políticas y medidas que permitan a las empresas acreditar el cumplimiento del marco legislativo desde el momento en el que se diseña un nuevo producto o servicio que implique un tratamiento de datos. Persigue además obtener una ventaja económica para las empresas, al permitir identificar, corregir y/o mitigar en las etapas iniciales del diseño de un nuevo producto o servicio, posibles riesgos que puedan derivarse de la misma antes de que el sistema se desarrolle, lo que implica, una solución de elevados costes para las empresas por el rediseño y adaptación de la tecnología. [18]

La implementación de estos principios exigirá que la protección de datos se integre en todo el ciclo de vida de cualquier producto o servicio a través del que se realice un tratamiento de datos personales, desde la primera fase de diseño hasta su despliegue final, su utilización y su eliminación definitiva, centrándose sistemáticamente en proporcionar amplias garantías respecto de la exactitud, la confidencialidad, la integridad, la seguridad física y la supresión de los datos personales. [18]

El Responsable del tratamiento deberá diseñar las operaciones de tratamiento implementando medidas técnicas y organizativas adecuadas para garantizar que el interesado pueda ejercer sus derechos.

Si bien no están definidos como derechos del interesado, el Reglamento dispone que el interesado da su consentimiento explícito para tratar sus datos, por lo que el diseño del tratamiento también debe incorporar soluciones para:

- **Revocación**: Retirar en cualquier momento el consentimiento dado, sin que afecte al tratamiento efectuado hasta entonces. Debe ser tan fácil retirar el consentimiento como el haberlo dado.
- **Reclamación**: Informar del derecho a presentar una reclamación ante la Autoridad de control si considera que el tratamiento no se ajusta al Reglamento.[16]

De lo anterior surge la implementación de lo que se denomina el **Derecho al olvido**:

> El nuevo paquete de protección de datos dispone que cada individuo tiene derecho a solicitar la rectificación o supresión de su información personal [20]

1.2.10. Delegado de Protección de Datos – DPO

El Reglamento dedica toda la Sección 4 del Capítulo IV al Delegado de Protección de Datos especificando sus cometidos, funciones y la obligatoriedad para designarlos (artículos 37 a 39).

El DPO es la persona encargada de informar y asesorar al Responsable o Encargado del tratamiento y al personal autorizado para

el tratamiento, de las obligaciones que les afectan en virtud del Reglamento (GDPR) y de cualquier otra disposición legislativa de protección de datos vigente en la UE o en los Estados miembros de la UE.

Para cumplir este cometido, el DPO se encargará de supervisar:

- La implementación y aplicación de las políticas de protección de datos.
- La asignación de responsabilidades, concienciación y formación del personal autorizado.
- La realización de la evaluación de impacto.
- Las auditorías realizadas.

Cualquier Responsable o Encargado del tratamiento o asociación u organismo que los represente, podrán designar un DPO y autorizarlo para actuar por su cuenta. Se podrá nombrar un único DPO para varios Responsables o Encargados del tratamiento cuando se designe para representar a:

- Un grupo de empresas, siempre que sea accesible desde cada uno de los establecimientos del grupo.
- Varias entidades de un mismo Organismo público, siempre que se tenga en cuenta su estructura organizativa y su tamaño.

El DPO actuará como punto de contacto o de consulta con la Autoridad de control y deberá cooperar con ella.

1.2.10.1 ¿Quién puede ser DPO?

Un DPO puede ser cualquier persona que pertenezca a la plantilla del Responsable o Encargado del tratamiento o, si es externo, en el marco de un contrato de servicios.

El DPO será designado atendiendo a:

- Cualidades profesionales.
- Conocimientos especializados en protección de datos.

- Capacidad para ejecutar los cometidos que le confiere el Reglamento.

El Responsable o Encargado del tratamiento deberán publicar los datos de contacto del DPO y comunicarlos a la Autoridad de control.

1.2.10.2. Funciones del DPO

El Delegado de Protección de Datos:

- Desempeñará sus cometidos prestando la debida atención a los riesgos en la protección de datos, teniendo en cuenta la naturaleza, alcance, contexto y fines del tratamiento.
- Estará obligado a mantener el secreto o la confidencialidad de sus cometidos.
- Podrá desempeñar otros cometidos y funciones ajenas a su relación con el Responsable o Encargado del tratamiento, siempre que no exista un conflicto de intereses con los mismos.
- Podrá informar directamente al más alto nivel de dirección del Responsable o Encargado del tratamiento.

Los Responsables o Encargados del tratamiento deberán:

- Respaldarle para que pueda cumplir sus cometidos.
- Facilitarle los recursos necesarios para desempeñar sus funciones y mantener sus conocimientos especializados.
- Velar para que el DPO no reciba ninguna instrucción en lo que respecta al ejercicio de sus cometidos y no podrán destituirle ni sancionarlo por realizarlos.

Los interesados podrán contactar con el DPO para tratar los asuntos que les afecten relativos al tratamiento de sus datos y al ejercicio de los derechos que les confiere el Reglamento.

1.2.10.3. ¿Cuándo existe la obligación de designar un DPO?

El Responsable o Encargado del tratamiento están obligados a designar un DPO **cuando su actividad principal contemple tratamientos a gran escala** de:

- **Observación habitual y sistemática de interesados**: Cuando se realiza un seguimiento frecuente y repetitivo de personas mediante un método de organización, clasificación u ordenación de sus datos.

  ***Por ejemplo**: Banca, Aseguradoras, Empresas de vigilancia que traten datos directamente como ET, Empresas dedicadas a la elaboración de perfiles (ETT, Mercadotecnia directa, Apps, etc.), Medios de comunicación, etc.*
- **Categorías especiales de datos**: Datos relativos al origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos que permitan la identificación unívoca de una persona, datos relativos a la salud o a la vida y orientación sexuales.

  ***Por ejemplo**: Partidos políticos, Iglesias, Sindicatos, Investigación genética o biométrica, Hospitales, Centros médicos, Mutuas, Asistencia social, etc.*
- **Datos relativos a condenas e infracciones penales**: Datos relativos a condenas e infracciones penales o medidas de seguridad afines, llevadas a cabo bajo la supervisión de autoridades públicas.

  ***Por ejemplo**: Gabinetes jurídicos.*

También existe la obligación de designar un DPO **cuando el tratamiento lo realice una Autoridad u Organismo público**, excepto los tribunales que actúan en el ejercicio de su función judicial.

1.2.11. ¿Cuándo una actividad principal contempla tratamientos a gran escala?

Vista la obligación establecida en el Reglamento para designar un DPO, esta figura sólo será necesaria en empresas que realicen

tratamientos de datos personales a gran escala en su actividad principal. La mayoría de empresas no realizan este tipo de tratamiento, por lo que podrán prescindir del DPO.

Del Artículo 91 (tratamientos a gran escala) y articulo 97 (actividad principal) del GDPR se desprende:

- **Tratamientos a gran escala**: Operaciones de tratamiento que persiguen tratar una cantidad considerable de datos personales que afectan a un gran número de ciudadanos con la probabilidad de existir un alto riesgo para los derechos y libertades de los mismos.
- **Actividad principal del Responsable o Encargado del tratamient**o: A lo que se dedica la empresa, su actividad económica. Por ejemplo, en una fábrica de calcetines la actividad principal es su fabricación y venta; en una empresa de trabajo temporal (ETT) su actividad principal es elaborar perfiles de personas para proporcionarles un empleo. Es muy importante discernir si la actividad principal se basa, o no, en el tratamiento de datos personales.[14]

Por lo visto, el perfil del DPO será un nuevo rol con el cual tendrán que contar gran parte de las organizaciones que trabaje con datos personales. Sin ir más lejos, un dentista que recolecta información sanitaria de sus pacientes (datos de tratamiento especial) deberá tomar sus recaudos y disponer de alguien con este rol. Por lo tanto, queda en evidencia que el DPO se convertirá en una nueva profesión indispensable que demandará constante entrenamiento, capacitación y certificación para desarrollarse como es esperado.

1.2.12. Autoridad de control

La normativa establece la creación de una autoridad pública independiente (artículo 4, apartado 21) definida por un Estado miembro de la Unión Europea con el fin de:

- Supervisar la correcta aplicación de la reglamentación a fin de proteger los derechos y libertades fundamentales de las personas

físicas en referencia al tratamiento de sus datos personales y a facilitar la libre circulación de datos dentro de la Unión Europea.

- Cooperar con otras Autoridades de control y la Comisión Europea a fin de contribuir a la coherente aplicación de la normativa.
- Si existieran varias autoridades de control para un estado de la Unión Europea, se designará una que las represente ante el Comité Europeo.

1.2.13. Funciones que afectan al Responsable y al Encargado del tratamiento:

- Recibir las notificaciones de violaciones de seguridad del Responsable del tratamiento y, si procede, exigir su comunicación al interesado.
- Adoptar cláusulas contractuales tipo de protección de datos para:
    - La formalización de contratos entre el Responsable y el Encargado del tratamiento.
    - Realizar transferencias internacionales de datos mediante garantías adecuadas.
    - Autorizar las cláusulas contractuales establecidas entre el Responsable del tratamiento, Encargado del tratamiento o Destinatarios para realizar transferencias internacionales de datos.
    - Elaborar y mantener una lista de los tipos de tratamiento que requieren una evaluación de impacto y de los detalles que se deben incluir en su documentación.
    - Asesorar al Responsable o al Encargado del tratamiento del procedimiento para realizar una consulta previa a la Autoridad de control y, cuando ésta se haya producido y no sea conforme al Reglamento, comunicárselo por escrito en un plazo máximo de 8 semanas.

1.2.13.1. **Funciones que afectan a las garantías de cumplimiento:**

- Establecer los requisitos de certificación y expedir los mecanismos de certificación, sellos y marcas de protección de datos a los Responsables

o Encargados del tratamiento que lo soliciten y renovarlos o retirarlos a su vencimiento.

- Elaborar y publicar los criterios para la acreditación de un organismo de certificación o de supervisión de códigos de conducta y expedir la acreditación a tales organismos.
- Emitir un dictamen y aprobar los proyectos de códigos de conducta presentados por asociaciones y organismos que representen a categorías de Responsables o Encargados del tratamiento.
- Aprobar las normas corporativas vinculantes solicitadas por grupos empresariales o por la unión de empresas dedicadas a una actividad económica conjunta que realicen transferencias internacionales de datos.

1.2.14. Poderes de la Autoridad de control

Cada Autoridad de control dispondrá de los siguientes poderes investigadores:

- Ordenar al Responsable y al Encargado del tratamiento o, si lo hubiere, al representante de estos, que faciliten cualquier información que requiera para el desempeño de sus funciones.
- Llevar a cabo investigaciones en forma de auditorías de protección de datos.
- Llevar a cabo una revisión de las certificaciones expedidas.
- Notificar al Responsable y al Encargado del tratamiento las presuntas infracciones del Reglamento.
- Obtener del Responsable y del Encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones.
- Obtener el acceso a todos los locales del Responsable y del Encargado del tratamiento, incluidos cualquiera de los equipos y medios de tratamiento de datos.

1.2.14.1. Cada Autoridad de control dispondrá de los siguientes poderes correctores:

- Formular advertencias o amonestaciones al Responsable y al Encargado del tratamiento cuando las operaciones de tratamiento puedan infringir el Reglamento.
- Ordenar al Responsable y al Encargado del tratamiento que atiendan las solicitudes del interesado para ejercer sus derechos con arreglo al Reglamento.
- Ordenar al Responsable y al Encargado del tratamiento que realicen el tratamiento en consonancia con el Reglamento, en una forma y plazo especificado.
- Ordenar al Responsable del tratamiento la comunicación de una violación de seguridad a los interesados afectados por la misma.
- Imponer una limitación temporal o definitiva del tratamiento.
- Ordenar la rectificación, limitación o supresión de datos.
- Retirar una certificación si no se cumplen los requisitos legales.
- Imponer una multa administrativa según las circunstancias de cada caso particular.
- Ordenar la suspensión de una transferencia internacional de datos.

1.2.15. **Derechos**

1.2.15.1 Derecho a presentar una reclamación ante la Autoridad de control

Todo interesado podrá reclamar ante la Autoridad de control de cualquier Estado de la UE, si considera que el tratamiento de sus datos personales no se ajusta a lo dispuesto en el Reglamento.

1.2.15.2 Derecho a un recurso judicial contra una Autoridad de control

- Los Responsables o Encargados del tratamiento tendrán derecho a un recurso judicial efectivo contra una decisión jurídicamente vinculante de la Autoridad de control que les afecte.
- El interesado tendrá derecho a un recurso judicial efectivo en contra de la Autoridad de control cuando ésta no de curso a una reclamación o no le haya informado en 3 meses.

1.2.15.3. Derecho a un recurso judicial contra un Responsable o Encargado del tratamiento

- El interesado tendrá derecho a un recurso judicial efectivo contra un Responsable o Encargado del tratamiento cuando considere que el tratamiento de sus datos personales no se ajusta a lo dispuesto en el Reglamento.
- Las acciones contra el Responsable o Encargado del tratamiento podrán ejercitarse ante los órganos jurídicos del Estado de la UE donde:
    - Esté establecido el Responsable o el Encargado del tratamiento.
    - Resida el interesado, siempre y cuando el Responsable o Encargado del tratamiento no sea una Autoridad pública que actúe en ejercicio de su poder público.

1.2.15.4. Derecho a indemnización y responsabilidad

Todo interesado que haya sufrido perjuicio material o inmaterial como consecuencia de una vulneración del Reglamento, tendrá derecho a recibir una indemnización del Responsable o del Encargado del tratamiento.

- Si los responsables o encargados participan en el mismo tratamiento, cada responsable o encargado debe ser considerado responsable de la totalidad de los daños y perjuicios. No obstante, si se acumulan en la misma causa, la indemnización puede prorratearse en función de la responsabilidad de cada responsable o

encargado por los daños y perjuicios causados por el tratamiento, siempre que se garantice la indemnización total y efectiva del interesado que sufrió los daños y perjuicios. En este caso, todo responsable o encargado que haya abonado la totalidad de la indemnización puede interponer recurso posteriormente contra otros responsables o encargados que hayan participado en el mismo tratamiento

- El Encargado del tratamiento solo será responsable de los perjuicios provocados por el tratamiento cuando haya actuado al margen o en contra de las instrucciones legales del Responsable del tratamiento o haya incumplido las obligaciones que le impone Reglamento.
- Los Responsables o Encargados del tratamiento estarán exentos de responsabilidades si consiguen probar que no son responsables del hecho que ha provocado el perjuicio.

1.2.15.5. Derecho a la representación del interesado

El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin afán de lucro correctamente constituida, cuyos objetivos estatutarios sean de interés público y actúen en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presenten una reclamación en su nombre y que ejerzan los derechos de:

- Recurso judicial contra una Autoridad de control.
- Recurso judicial contra un Responsable o Encargado del tratamiento.
- Indemnización y responsabilidad. [13]

1.2.16. Multas

Las empresas se sentirán mucho más motivadas a cumplir las nuevas normas, debido a las multas notablemente más altas, que alcanzan hasta el 4% del volumen de negocios mundial del año fiscal

precedente, o 20 millones de euros (lo que sea mayor), por graves incumplimientos de los principios del GDPR.

Asimismo, un estudio de Veritas establece que el 18% de las empresas a nivel mundial temen dejar de operar por el incumplimiento de la nueva reglamentación debido a las elevadas multas. [12], el 21% de las mismas consideran elevados los montos de las sanciones económicas y afirman que potencialmente podría implicar recortes y despidos.

1.2.16.1. Valoración de las sanciones

La decisión de la Autoridad de control para imponer una multa administrativa y calcular su importe tendrá en cuenta:

- La naturaleza, gravedad y duración de la infracción en relación con el fin del tratamiento.
- El número de interesados afectados.
- El nivel de los perjuicios sufridos por los interesados.
- La intencionalidad o negligencia de la infracción.
- Las categorías de datos afectados por la infracción.
- El grado de responsabilidad del Responsable o Encargado del tratamiento.
- La reiteración de infracciones del Responsable o Encargado del tratamiento.
- Las medidas tomadas por el Responsable o Encargado del tratamiento para paliar los perjuicios sufridos por los interesados.
- El grado de cooperación con la Autoridad de control con el fin de remediar la infracción y mitigar sus posibles efectos adversos.
- La forma en que la Autoridad de control ha tenido conocimiento de la infracción (si se ha notificado, o en la medida que se ha hecho).
- El cumplimiento de las medidas ordenadas previamente por la Autoridad de control contra el Responsable o Encargado del tratamiento en relación con el mismo asunto.

- La adhesión a códigos de conducta o a mecanismos de certificación aprobados por la Autoridad de control.
- Otros factores agravantes o atenuantes aplicables a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas por la infracción.

1.2.16.2 Importe de las sanciones

a) Multa administrativa con un máximo del importe más elevado entre **10.000.000 € y el 2% del volumen de negocio total anual global del ejercicio financiero anterior**, para las infracciones de las siguientes disposiciones del Reglamento:

- Condiciones aplicables al consentimiento del menor en relación con los servicios de la sociedad de la información.
- Tratamientos que no requieren identificación.
- Encargados del tratamiento.
- Corresponsables del tratamiento.
- Tratamientos bajo la autoridad del Responsable y del Encargado del tratamiento.
- Representantes de los Responsables del tratamiento no establecidos en la UE.
- Registro de las actividades del tratamiento.
- Protección de datos desde el diseño y por defecto.
- Seguridad del tratamiento.
- Evaluación de impacto relativa a la protección de datos.
- Consultas previas.
- Notificación de una violación de seguridad a la Autoridad de control.
- Comunicación de una violación de seguridad al interesado.
- Garantías de certificación.
- Organismos y procedimientos de certificación.
- Designación del DPO.
- Funciones del DPO.
- Poderes del DPO.

- Cooperación con la Autoridad de control.

b) Multa administrativa con un máximo del importe más elevado entre **20.000.000 € y el 2% del volumen de negocio total anual global del ejercicio financiero anterior**, para las infracciones de las siguientes disposiciones del Reglamento:
Principios relativos al tratamiento de datos personales.

- Licitud del tratamiento.
- Condiciones para el consentimiento.
- Tratamiento de categorías especiales de datos personales.
- Transferencias de datos personales a terceros países u organizaciones internacionales.
- Disposiciones relativas a situaciones específicas de tratamiento de datos.
- Derechos del interesado.
- No facilitar el acceso a la Autoridad de control para ejercer sus facultades investigadoras.
- El incumplimiento de un requerimiento de la Autoridad de control.

c) Multa administrativa con un máximo del importe más elevado entre **20.000.000 € y el 4% del volumen de negocio total anual global del ejercicio financiero anterior**, para las infracciones de las siguientes disposiciones del Reglamento:

- El incumplimiento de las resoluciones de la Autoridad de control.

El importe total de las multas para las mismas operaciones de tratamiento que incumplan diversas disposiciones del Reglamento, no podrá superar la cantidad prevista para los incumplimientos más graves de dichas operaciones.

Cada Estado de la UE podrá establecer normas sobre la imposición de multas administrativas a las Autoridades y Organismos públicos establecidos en dicho Estado. [13]

1.2.17. Transferencias internacionales de datos

En el capítulo 5 de la normativa se tratan las condiciones para efectuar transferencias de datos a terceros países u organizaciones, entre las cuales se establece que debe existir un permiso de la Comisión Europea para efectuar dicha operación hacia este país manteniendo las garantías adecuadas para la protección de los datos a transferir.

1.2.18. Documentación para garantizar la correcta aplicación de GDPR

El Reglamento dispone de varios mecanismos para garantizar que se han implementado medidas adecuadas de protección de datos y acreditar su cumplimiento. Dichas garantías pretenden incrementar la confianza y la transparencia de las actuaciones llevadas a cabo con datos personales por Responsables y Encargados del tratamiento.

Las garantías de cumplimiento que prevé la reglamentación son:

- **Mecanismos de certificación**: Para Responsables o Encargados del tratamiento a título individual (Certificados, Sellos y Marcas de protección de datos).
- **Códigos de conducta**: Para asociaciones u organismos que representen categorías de Responsables o Encargados del tratamiento.
- **Normas corporativas vinculantes**: Para grupos empresariales o unión de empresas dedicadas a una actividad económica conjunta que realicen transferencias internacionales de datos.

Cualquier Responsable o Encargado del tratamiento también podrá emitir por su cuenta un certificado que garantice el cumplimiento de las disposiciones establecidas en el Reglamento.

Figura 4- Documentación para garantizar la aplicación de GDPR [17]

Para ello, se deberán crear diversos protocolos de actuación con el fin de poder garantizar la protección de datos en todas las fases del tratamiento:

- **Principios del tratamiento** (responsabilidad proactiva).
- **Responsabilidad del tratamiento** (registro de las actividades).
- **Política de información** (información y comunicación al interesado).
- **Política de seguridad** (análisis de riesgos y evaluación del impacto).
- **Medidas de protección de datos** (actuaciones específicas de seguridad).

1.3 Predicciones y estadísticas

Con todos estos cambios que parecen favorecer al usuario, “casi la mitad de las organizaciones y empresas de más de 1.000 empleados en todo el mundo (un 47%) consideran que no están preparadas para cumplirla dentro de los plazos con los requisitos que establece”. [10]
A su vez, un estudio efectuado por Veritas Technologies, manifiesta que “el 86 por ciento de las empresas consultadas creen que no cumplir con el nuevo reglamento puede tener consecuencias negativas en sus negocios” [11]

Un estudio[12] efectuado por NetApp, asegura que “más del 70 % de las organizaciones manifiesta tener cierto grado de preocupación por cumplir la normativa dentro del plazo estipulado” pero “solo el 37% de los encuestados asegura haber destinado fondos adicionales a garantizar la adecuación a la normativa”.

Por otra parte, el mismo estudio establece que “el 51% de los encuestados afirma que la responsabilidad de la adecuación a la normativa corresponde a la compañía que produce los datos; el 46% considera que recae en la compañía que los procesa; y por otra parte, el 37% cree que la responsabilidad recae en los proveedores externos de servicios en la nube”. Cabe destacar en este punto que de acuerdo a la ley, todas las partes mencionadas tienen responsabilidad individual sobre los datos que gestionan.

Del mismo estudio, surge que “Alemania demuestra ser el territorio mejor informado al respecto, y sin embargo, solo el 17% de los encuestados asegura comprender la nueva normativa en toda su extensión. Francia se sitúa segunda, con un 15%, seguida del Reino Unido, con un 12%. La mayoría de los encuestados asegura tener una noción “parcial” del GDPR (un 47%). Con apenas un año por delante para garantizar la conformidad con la normativa, el 9% de los encuestados asegura no saber qué es el GDPR.”[12]. Ver Fig. 2 en el Anexo.

1.4 Costos estimados de implementación

En términos de gastos e impacto microeconómico, las empresas deberán desembolsar grandes sumas de dinero para poder alinearse con la nueva normativa.

Según un estudio de TrustArc,[34] el 83% de los profesionales de seguridad en EEUU estiman destinar por lo menos U$D100.000 , de los cuales 17% planea asignar más de un millón de dólares. Por otro lado, el 40 % de las compañías estima que el costo de ser compatible con esta nueva normativa será de por lo menos medio millón de dólares. Teniendo en cuenta que al momento del estudio, el 61 % de la compañías no habían comenzado la implementación aun de ninguna medida para acatar la nueva reglamentación y el 43% no tenía un plan completamente definido.

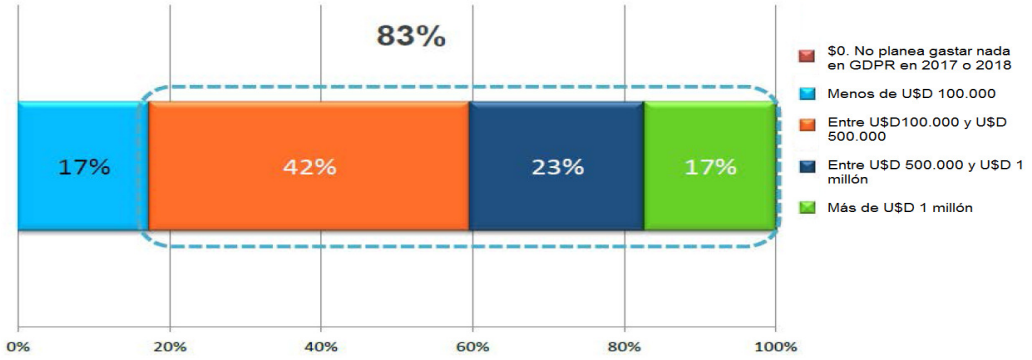


Fig. 5 – Gasto estimado en GDPR

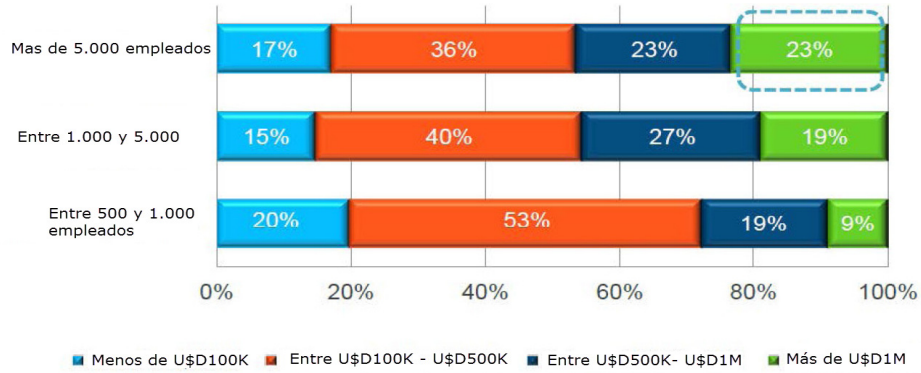


Figura 6 - Gasto estimado por tamaño de la organización: Según el estudio de TrustArc[34], el 9% de las compañías pequeñas y el 19% de las mediana planean gastar más de un millón de dólares en iniciativas relacionas a GDPR.

Por otro lado, existe aún cierta resistencia y temas por resolver. Por ejemplo. la implementación de la normativa al restringir la recopilacion de informacion plantea un serio inconveniente para las consecución de alertas de los sistemas de Lavado de Dinero (AML Anti-money laundering) realizados por las entidades financieras y bancarias a nivel mundial. Por lo tanto, las entidades financieras se encontrarán limitadas de almacenar y recopilar informacion con fines de identificación de anomalias y operaciones sospechosas en el sistema financiero[35].

2. Comparación con políticas generales de Estados Unidos

Como consecuencia de la globalización, la cooperación entre los Estados es algo habitual y lógico. Sin embargo, a veces puede resultar complicada la cooperación entre estados que disponen diferente legislación y ordenamiento jurídicos. Generalmente estas diferencias son salvadas mediante acuerdos y tratados internacionales.

Las diferencias entre Europa y Estados Unidos son significativas tanto a nivel normativo como a nivel ideológico.

Mientras que en Europa se tiende a confiar en el estado, en Estados Unidos se tiende a confiar en el individuo intentando limitar al máximo la intervención del gobierno y reservándolo para pocas excepciones. [25]

Estados Unidos dispone de diferentes leyes y políticas aplicadas a lo largo de sus 50 estados (por ejemplo, California dispone de más de 25 leyes estatales sobre privacidad y privacidad de los datos).

Cada una de estas leyes se focaliza en casos particulares o industrias particulares, por lo que resulta muy difícil generalizar las políticas aplicadas dentro de este país.

Sin embargo, gran parte de las compañías se encuentran reguladas por la FTC ("Federal Trade Commission"[1]) quien en varias ocasiones promovió las buenas prácticas y políticas de protección de datos personales.

2.1. Definición de dato personal.

[1] Comisión Federal de Comercio (Federal Trade Commission o FTC) es una agencia independiente del gobierno de los Estados Unidos, establecida en 1914 por el Acta de la Comisión Federal de Comercio (Federal Trade Commission Act). Su misión principal es promover los derechos de los consumidores y la eliminación y prevención de prácticas que atentan contra la libre competencia. Fuente: https://es.wikipedia.org/wiki/Comisi%C3%B3n_Federal_de_Comercio, consultada 13/8/2017

Para establecer una clara diferencia entre ambas legislaciones, debemos partir de la definición que tienen ambas naciones sobre datos personales.

En el caso de Estados Unidos, la FTC considera **datos personales** a *información que puede ser utilizada para contactar, o distinguir a una persona incluyendo direcciones IP e identificadores de dispositivo*. Sin embargo algunas leyes federales o estatales definen "datos personales" a *cualquier información que le pertenece a la persona sin importar si esta la identifica o no*.

Por otro lado, la legislación define **datos personales sensibles** a la *información relacionada a la salud, finanzas, crediticia, académica datos personales recolectados en forma online de niños menores de 13 años,* información que puede ser utilizada para robar nuestra identidad o actuar fraudulentamente.

Cabe destacar que en este país no existe una autoridad nacional de protección de datos, aunque la FTC usualmente termine actuando como tal para asegurar que las operaciones se lleven a cabo bajo las condiciones adecuadas.

Si bien esto último se aplica en general, encontramos que en particular el estado de Massachusetts, dispuso una ley que obliga a las compañías que almacenan datos personales de residentes del estado a asignar uno o dos empleados para mantener el sistema de seguridad.

2.2. Recolección y procesamiento

Como ya fue indicado anteriormente, las políticas de los estados en Estados Unidos son muy diferentes entre sí. Sin embargo, en general es requerida una notificación previa a la recolección y uso de la información personal.

La reglamentación define que en casos especiales como información de niños menores de 13 años, reportes crediticios, información

académica o información de salud, será necesario un consentimiento explícito.

2.3 Transferencia de datos

No existen restricciones en la transferencia de datos en todo el territorio de los Estado Unidos excepto en los casos que la información sea gubernamental.

2.4. Seguridad

La mayoría de las industrias requieren tomar medidas razonables para proteger y garantizar la seguridad de los datos personales sensibles (por ejemplo regulado por legislaciones como la HIPAA - Health Insurance Portability and Accountability Act of 1996, legislación sobre datos médicos-, o el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago -Payment Card Industry Data Security Standard-). Sin embargo, algunos estados disponen de leyes más específicas que obligan a las compañías a notificar sobre los incidentes de seguridad a los individuos afectados. Por su parte, los estados de Massachusetts y Nevada han establecido políticas que exigen encriptar previamente los datos personales para transmitirlos a través de redes inalámbricas o para transportarlos en laptops u otros dispositivos portátiles.

2.4.1. Notificación de incumplimientos de seguridad

Estados Unidos es pionero en la notificación de los incumplimientos de seguridad. La mayoría de los estados exige la notificación de incidentes de seguridad que involucren residentes en los cuales esté comprometida información sensible como números de seguridad social, otras identificaciones gubernamentales, números de tarjetas de crédito, números de cuentas bancarias e información financiera. [26]

Para la ley estadounidense los tiempos de notificación son más flexibles que en GDPR. El texto de la GDPR establece “sin demora alguna”. En cambio en Estados Unidos aunque algunos estados definieron plazos de entre 2 y 90 días (lo más común es de 30 a 45 días). Por su parte, como se menciona anteriormente, GDPR exige la notificación a la autoridad de control inmediatamente y dentro de las 72 hs. del descubrimiento del incidente.

A su vez, las políticas del país norteamericano requieren menor granularidad de detalle en la notificación, ya que establece que la notificación debe contener una descripción del incidente, la información afectada y las medidas implementadas. Mientras que GDPR requiere documentación explicita para formalizar la notificación y permitir a la autoridad de control auditar el evento.

2.5 Comparación de políticas

En la tabla a continuación se puede apreciar sintéticamente una comparación de las diferencias generales en la legislación de la Unión Europea y los Estados Unidos.

Criterio	EEUU	Unión Europea
Ámbito legal	Normativas sectoriales por industria	Reconocido por muchas constituciones
Autoridad que controle el cumplimiento	No	Si
Tipo de enfoque	Reactivo. Se resuelve todo en los tribunales y si es necesario se compensa posteriormente	Preventivo
¿A quién protege?	Ciudadanos americanos	Todos los residentes de la unión europea sean ciudadanos o no
Recolección de datos	Sin restricciones, salvo excepciones o casos especiales (por ejemplo, datos de menores de edad)	Solo lo indispensable e imprescindible
Perspectiva de los ciudadanos	Se confía en el mercado (enfoque liberal en el cual el mercado se auto regula)	Se confía en el gobierno/ estado (enfoque paternalista)
Sanciones	No hay sanciones tasadas y se ve caso por caso	Tasadas. Pueden llegar a ser sumamente elevadas e incluir delitos penales
Alcance	Nombre, identificación gubernamental personal (SSN[2]), etc. + información de cuentas financieras (incluso usuario y contraseña en algunos estados)	Toda información que identifique o permita identificar a una persona
Definición de incidente	Acceso no autorizado o sustracción de información	Hubo una (accidental o no) destrucción, pérdida, alteración, uso no autorizado o acceso a datos personales transmitidos, almacenados o procesados

Tabla 1. Comparativa de políticas GDPR vs EEUU

Cabe destacar en esta instancia que para poder compatibilizar ambas legislaciones ambos gobiernos concertaron un acuerdo llamado “Privacy Shield” (Escudo de seguridad) para regular la protección de

[2] Social Security Number, número del seguro social que identifica a cada ciudadano estadounidense.

datos de personas europeas en la prestación de servicios que suponen transferencia internacional.[27]

Este nuevo acuerdo viene a sustituir al “Safe Harbour” que fue anulado por el Tribunal de Justicia de Unión Europea en octubre de 2015 por no garantizar el suficiente nivel de protección establecido.

2.6. Certificaciones

Este acuerdo, Privacy Shield, se fundamenta en establecer un sistema de auto-certificación mediante el cual las empresas de EEUU se comprometen a cumplir un conjunto de principios de privacidad, así como en su revisión conjunta entre la Comisión Europea y el Departamento de Comercio de EEUU, en colaboración con las entidades de control y protección de datos de los estados miembros de la Unión Europea.

Esto implica que las empresas europeas que transfieran datos de usuarios europeos a empresas en Estados Unidos no tendrán que solicitar autorización previa a la Agencia de Protección de Datos sino verificar que la empresa a la que transfieren datos haya adherido al acuerdo y comunicar la transferencia.

Para poder formar parte de la lista de organizaciones que cumplimentan el acuerdo se debe cumplir con los siguientes principios:

1. Principio de notificación y opción: Proporcionar información a los usuarios en sus políticas de privacidad sobre el tratamiento de los datos personales (tipo de datos recopilados, finalidad del tratamiento, el derecho de acceso y de oposición, las condiciones para las transferencias posteriores, el régimen de responsabilidad, etc.).
2. Limitar el almacenamiento y tratamiento de datos a lo estrictamente relevante y compatible con la finalidad para la que fueron recabados, conforme al consentimiento prestado por el titular de los datos.

3. Garantizar la obtención del consentimiento expreso y explícito en sentido afirmativo a la finalidad concreta por parte del titular de los datos
4. Conservar los datos sólo durante el tiempo que sirve a la finalidad para la que fueron inicialmente recogidos o autorizados.
5. Tomar las medidas de seguridad técnicas y organizativas "razonables y adecuadas" a la recogida de datos, su almacenamiento y tratamiento, teniendo en cuenta los riesgos involucrados en el tratamiento y la naturaleza de los datos.
6. Firma de contrato con el encargado de tratamiento de datos en el caso de cesión de los mismos con dicha finalidad
7. Garantizar el derecho de acceso al titular de los datos, así como a la corrección, modificación y eliminación de información personal inexacta o tratada en incumplimiento de los principios establecidos en el acuerdo. [27]

3. Comparación con políticas generales de Canadá – PIPEDA.

En Canadá hay 28 estatutos federales, provinciales y territoriales que regulan la protección de la información personal en los sectores públicos, privados y de salud.

La normativa principal y más reciente es PIPEDA, ("Personal Information Protection and Electronic Documents Act") aplicada al sector privado.

3.1 Alcance de PIPEDA

La normativa impacta:

- ✓ A las prácticas sobre información personal de consumidores y empleados de las organizaciones gubernamentales o corporativas (por ejemplo, bancos, empresas de telecomunicaciones, líneas aéreas, ferrocarriles y otros),
- ✓ Organizaciones que recopilan, utilizan y procesan información personal como parte de una actividad comercial,
- ✓ A la recolección, uso y divulgación de información personal inter provinciales e internacionales.

Para entender mejor la diferencia con la normativa GDPR es importante comenzar con la definición de datos personales según esta ley. PIPEDA define "información personal" como *cualquier información de un individuo fácilmente identificable*. La misma no hace referencia a una definición específica de datos sensibles como lo hace la reglamentación europea. Sin embargo, sí define la figura de una autoridad de control de protección de datos personales a nivel nacional llamado Oficina del comisionado de privacidad de Canadá ("Office of the Privacy Commissioner of Canadá")

Otra diferencia evidente entre ambas reglamentaciones se encuentra en el alcance de aplicación. Por ejemplo PIPEDA no es aplicable a los buscadores ya que la actividad de indexado de contenido de sitios web y la función de búsqueda no son consideradas actividades comerciales.

3.2 Recolección y procesamiento

Dependiendo de la sensibilidad de la información personal, el consentimiento puede ser requerido y la opción de solicitar que los datos sean borrados de la base de datos debe ser posible. Las organizaciones deben limitar la recolección de información personal y solo almacenar la información indispensable para el propósito que es recabada y retenerla estrictamente por el tiempo que la misma es necesaria brindando al individuo transparencia sobre el propósito y periodo de uso de sus datos personales. PIPEDA al igual que GDPR establece el derecho de acceso a la información personal almacenada con ciertas excepciones y el derecho del individuo de solicitar que la misma sea corregida y actualizada.

Sin embargo, PIPEDA solo brinda a los canadienses el derecho a saber qué información se tiene de ellos y GDPR va más allá, permitiéndole a la persona trasladarla a otro lugar (portabilidad).

También, es necesario mencionar que PIPEDA no presenta restricciones en cuanto a la edad del individuo que brinda el consenso. La Oficina del comisionado de privacidad de Canadá ha sugerido que el consenso de menores de 13 años es difícil de gestionar. Sin embargo no existen estrictas restricciones de rango de edad en este sentido.

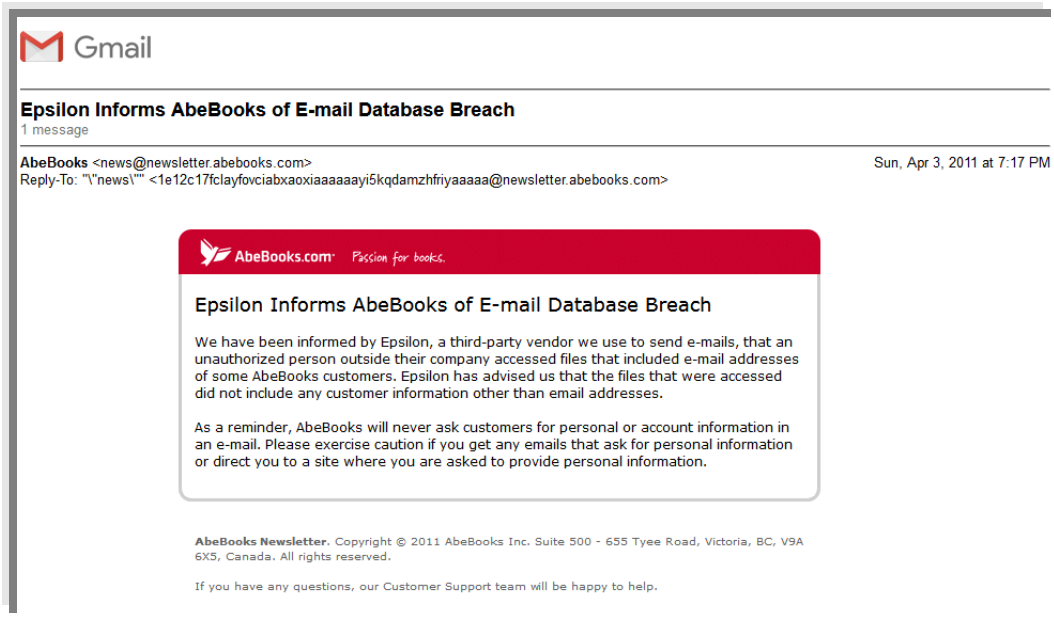
En cambio, GDPR define que el consentimiento será válido solo proviniendo de mayores de 16 años y en algunos casos excepcionales de mayores de 13 años.

3.3. Notificaciones

En términos de notificaciones, y a diferencia de GDPR, PIPEDA exige la notificación de incidentes a la Oficina del comisionado de privacidad de Canadá (“Office of the Privacy Commissioner of Canadá”) y en ciertos casos a los individuos afectados.

La misma debe contener:

- Una descripción de las circunstancias del incidente (pérdida de información o acceso no autorizado),
- Fecha o período durante el cual ocurrió el incidente,
- Descripción de la información personal involucrada (pérdida o a la cual se tuvo acceso),
- Evaluación de los riesgos y daños a los individuos involucrados,
- Un estimado del número de individuos impactados por el incidente a quienes este incidente les ocasionará daño inminente,
- Descripción de las medidas tomadas por la organización para minimizar el riesgo de daños a los individuos afectados,
- Descripción de los procedimientos de notificación a los individuos afectados,
- Nombre e información de contacto del responsable en la compañía ante la entidad para responder preguntas sobre el incidente.


Gmail

Epsilon Informs AbeBooks of E-mail Database Breach

1 message

AbeBooks <news@newsletter.abebooks.com> Sun, Apr 3, 2011 at 7:17 PM
Reply-To: "\"news\"" <1e12c17fclayfovciabxaoxiaaaaaayi5kqdamzhfriyaaaaa@newsletter.abebooks.com>

AbeBooks.com Passion for books.

Epsilon Informs AbeBooks of E-mail Database Breach

We have been informed by Epsilon, a third-party vendor we use to send e-mails, that an unauthorized person outside their company accessed files that included e-mail addresses of some AbeBooks customers. Epsilon has advised us that the files that were accessed did not include any customer information other than email addresses.

As a reminder, AbeBooks will never ask customers for personal or account information in an e-mail. Please exercise caution if you get any emails that ask for personal information or direct you to a site where you are asked to provide personal information.

AbeBooks Newsletter. Copyright © 2011 AbeBooks Inc. Suite 500 - 655 Tyee Road, Victoria, BC, V9A 6X5, Canada. All rights reserved.

If you have any questions, our Customer Support team will be happy to help.

Figura 6 – Ejemplo de notificación por mail a un cliente una vez ocurrida una violación de datos personales (Canadá). Abril/2011

En el caso de ser necesario notificar a las personas involucradas (cuando existen riesgos de daños) la ley exige incluir en las notificaciones:

- Descripción de las circunstancias del incidente,
- Fecha y período del mismo,
- Descripción de la información comprometida,
- Descripción de las medidas tomadas por la organización para minimizar el riesgo de daños a los individuos afectados,
- Nombre e información de contacto del responsable en la compañía para responder preguntas sobre el incidente.

A su vez, a diferencia de GDPR, PIPEDA carece de leyes que contemplen todos los aspectos de la privacidad. Por ejemplo, la privacidad del empleado no se encuentra protegida completamente salvos algunas jurisdicciones con políticas específicas para estos casos. [29]

En resumen, queda pendiente decidir si efectuarán una modificación a la actual ley Canadiense para adaptarse a las nuevas imposiciones de la reglamentación europea y alinearse con ellas.

Para ello se deberán incluir nuevas directivas que traten:

- Derecho al olvido
- Retención de datos
- Evaluaciones de impacto de la protección de datos
- Establecimiento de una oficina de representación en la unión europea
- Mayor detalle en las notificaciones
- Definición de sanciones
- Incorporación datos del empleado en la definición de datos personales
- Definición de las condiciones para la transferencia de datos

4. **GDPR y su impacto en Argentina**

La ley vigente de protección de datos personales en Argentina, ley 25.326 sancionada el 4/10/2000, se encuentra lejos de la nueva reglamentación europea. Sin embargo al momento de escribir el presente trabajo se ha podido acceder a un borrador de las propuestas de cambios a la ley actual con el propósito de alinearse con la normativa GDPR.[3]

Entre los cambios más llamativos se encuentra la eliminación de la necesidad de registrar bases de datos y el reconocimiento solo a los individuos como "sujetos de datos", mientras que la ley actual reconoce a "persona física o a persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país"(sic. Art 2 de la ley).

A su vez, la propuesta introduce la novedad de las definiciones de datos biométricos y datos genéticos. Asimismo, el borrador menciona métodos para determinar si el procesamiento de datos se encuentra acatado por la ley argentina o no, aplicando criterios similares a los que se aplican en GDPR.

También este nuevo documento trata temas como la necesidad explícita del consentimiento, transferencias internacionales, responsabilidades tales como la nominación de un DPO, efectuar evaluaciones periódicas de impacto y la implementación de privacidad desde el diseño entre otras que ya se han mencionado a lo largo de este trabajo.

- [3] http://www.jus.gob.ar/media/3210629/anteproyecto_de_ley_de_protecci_n_de_los_datos_personales.pdf

5. **Costos y cambios organizacionales asociados a GDPR**

Como ya se ha comentado el DPO representa un nuevo protagonista en la escena de la administración de los datos personales.

Como es evidente, esta nueva figura dentro de la empresa implicará cambios organizacionales desde culturales hasta económicos.

Para empezar, los profesionales deberán comenzar a capacitarse en diferentes temas relacionados a la privacidad de los datos personales y las tecnologías vigentes para entender y poder aplicar sus conocimientos al nuevo rol.

La nueva figura del DPO requerirá formación jurídica, técnica y multidisciplinaria simultáneamente. Por otro lado, ya comenzaron a surgir certificaciones y programas de entrenamiento que validan los conocimientos de quien desempeñe ese rol o desee hacerlo.

Estas certificaciones o programas sin duda traerán consigo costos asociados para la compañía, que a su vez se consideran parte de la inversión para lograr el completo alineamiento con la nueva reglamentación. Es preciso destacar que estas certificaciones son un instrumento indispensable para acreditar efectivamente los conocimientos necesarios para ocupar el nuevo rol.

Por otro lado, como ya fue mencionado, existe la posibilidad de tercerizar este rol y que una empresa externa lo ejerza, por lo que también implicará un desembolso mensual por parte de la corporación para poder asegurarse que cumple con las nuevas políticas. Si bien parece trivial, bajo esta modalidad existe un costo inherente que pocos tienen en consideración. El costo de entrenar a una nueva persona o grupos de personas para que entiendan los procesos de la compañía y qué se hace con la información (algo que es mucho más simple y rápido cuando el DPO se encuentra dentro de la compañía).

Este DPO externo puede que sea DPO de más de una compañía por lo que deberá ser muy metódico y atento a lo que ocurre en cada uno de sus “clientes”.

El rol del DPO entra al organigrama de la compañía impuesto por ley, y no va tomando preponderancia gradualmente hasta ser un eslabón crítico dentro de la cadena de mando, sino que abruptamente se incorpora reportando directo a la dirección de la compañía. El impacto cultural resultante que este cambio implica es de alta relevancia ya que repentinamente tomará un lugar de autoridad y podrá imponer sus ideas, cambios y nuevos requisitos dentro de los procesos vigentes de la empresa. Para lo cual la dirección corporativa deberá invertir en educar a toda la compañía sobre la importancia y lugar de esta nueva figura. No será una tarea fácil incorporar un nuevo "supervisor" sin una campaña de concientización previa.

Cabe destacar que un reciente estudio establece que para el momento de la implementación completa de la reglamentación, se requerirán al mercado 28.000 profesionales [40] que cuenten con los conocimientos necesarios para desempeñarse en sus roles. Con este pronóstico fácilmente se puede vaticinar la gran demanda de estos perfiles en términos de recursos humanos.

Si bien el artículo 37 de la reglamentación no especifica qué credenciales debe tener el DPO, es evidente que a partir de este nuevo rol comenzarán a surgir especializaciones, cursos de actualización y preparación para cumplir con las exigencias de este nuevo actor. Sin embargo, no cabe duda que el mismo requerirá capacidad de gestión e interacción con usuarios internos y externos de diferentes niveles de jerarquía así como también la capacidad de interactuar con autoridades gubernamentales y de control para responder ante auditorías o controles y reportar incidentes.

6. Compatibilidad con computación en la nube. ¿Son los requisitos de GDPR suficientes?

La computación en la nube es un modelo de acceso a los sistemas informáticos, en el que los datos y las aplicaciones están hospedados en Internet y en centros de cómputo remotos, de tal modo que pueden ser utilizados desde cualquier punto que tenga conexión a la red mundial. La computación en la nube permite que los consumidores y las empresas gestionen archivos y utilicen los programas, sin necesidad de instalarlos localmente en sus computadores. Esta tecnología ofrece un uso mucho más eficiente de los recursos, tales como almacenamiento, memoria, procesamiento y ancho de banda.

El término "nube" se utiliza como una metáfora de Internet, y se origina en la nube utilizada para representar Internet en los diagramas de red, como una abstracción de la infraestructura que representa. [28]

Las estadísticas indican que en 2017 el 21 % de las empresas europeas utilizaron servicios de computación en la nube durante el 2016, la mayoría de las cuales lo utilizaron solo para albergar su sistema de correo electrónico o almacenar archivos. [33]

Para una organización utilizando computación en la nube, existen varios aspectos de la normativa europea a los cuales deben prestar especial consideración para asegurar la compatibilidad con GDPR. Por su naturaleza, los datos almacenados en la nube son delegados a otra compañía subcontratada. Por lo tanto las compañías deben tomar precauciones y asegurarse de contratar a un proveedor que pueda garantizar el nivel adecuado de seguridad. [30]

La reglamentación exige a las organizaciones y proveedores de computación en la nube tomar las siguientes medidas:

- ✓ Proveedores de servicios en la nube tienen la obligación de:
- Garantizar el fácil cambio de proveedor de servicios,

- Reportar incidentes dentro de las 72 horas y presentar las evidencias de los mismos,
- Absoluta confianza de que los datos no serán procesados por el proveedor de servicios sin previa autorización de ambos, el cliente y la entidad de recolección de datos,
- Asegurar que la información se procesa de acuerdo a los procedimientos documentados.

✓ Del mismo modo, las compañías deberán brindar a los individuos:

- Asignación de un controlador de datos,
- Consentimiento explícito y claro del individuo para recolectar y procesar sus datos personales,
- El derecho al olvido en caso de ser requerido,
- La posibilidad de mover sus datos de un proveedor a otro con facilidad,
- Completa y concreta información de quién recolecta los datos sobre los procesos aplicados a la información recopilada,
- El derecho a ser notificado en caso de un incidente dentro de las 72 horas de ocurrido el mismo.

Para facilitar esto, la normativa permite a los proveedores de servicios de computación en la nube demostrar el cumplimiento de los requerimientos a través de la participación en procesos de certificación avalados por autoridades supervisoras o bien la adopción de códigos de conducta predefinidos.

Estas opciones a su vez, serán útiles para que los controladores puedan evaluar los diferentes proveedores y asegurar su correcta compatibilidad.[31]

6.1. La nube híbrida, una alternativa tentadora

Desde sus inicios, la computación en la nube ha demostrado ser tremendamente beneficiosa para todas las empresas, proporcionando computación flexible y potente, almacenamiento bajo demanda, y también fiabilidad y seguridad a las organizaciones. Sin embargo, con la entrada en vigor de la aplicación del nuevo reglamento de protección de datos de la UE, la nube híbrida, comienza a demostrar su verdadero valor y ventajas [32]

Figura 7 – Nube hibrida

Las organizaciones utilizan una nube híbrida para almacenar los datos más sensibles en la nube privada, más bloqueada y controlada, para darles una capa adicional de seguridad. Esto también facilita el trabajo con otras empresas, ya que puede bloquear algunos datos en la nube privada, y por otra parte compartiendo información esencial a través de la nube pública.

Por otro lado, con computación en la nube híbrida también es posible ejecutar dos nubes interconectadas, cada una almacenando y procesando diferentes conjuntos de datos. La combinación es potente, porque la nube pública aporta la escala y la eficiencia necesaria, mientras que la nube privada ofrece seguridad, velocidad y personalización.

La clave para sacar el máximo provecho de una nube híbrida es definir dónde dividir los datos y procesarlos. Según una investigación de IDC, las aplicaciones más probables de ser adoptadas por la nube pública incluyen redes sociales empresariales, correo electrónico, gestión de contenido web, pruebas y gestión de dispositivos móviles.

Sin embargo, cabe destacar que el desembolso inicial para implementar una nube híbrida puede ser alto; y su despliegue, complicado, particularmente cuando se implementan las interconexiones seguras entre las nubes

públicas y privadas. Aun así, esa inversión se pagará rápidamente por sí misma, haciendo a la empresa más flexible, fiable, segura y competitiva, y ayudando a evitar cuantiosas multas como consecuencia del incumplimiento del GDPR [32]

7. Medir y evaluar la efectiva implementación de GDPR: Verificación de compatibilidad con GDPR

El reloj empezó a contar y el momento se acerca. Las organizaciones deberán adecuarse a esta nueva regulación. El tiempo se acaba y cada entidad debe asegurarse de cumplir con la nueva política antes de mayo del 2018.

Por el momento no hay herramientas concretas de medición de compatibilidad con GDPR. Más bien han surgido desde la publicación de la ley, tutoriales que ayudan a identificar los potenciales cambios necesarios para llegar en tiempo y forma a la fecha límite y guían a las organizaciones en la adopción de GDPR.

Es por ello que, las diferentes consultoras y especialistas en el tema desarrollaron sus propias herramientas y documentos para ayudar simplificar el proceso de adecuación y brindar a sus clientes (o potenciales clientes) un marco de referencia desde el cual empezar. [42][43][44][45][46][47][48][49]

Cabe destacar que estos manuales intentan ser lo más abarcativos y generales posibles. Éstos se focalizan en mostrar que se debe cumplir más que en “cómo “se debe cumplir, dejando de lado cuestiones más específicas de cada industria y organización en particular.

En general estas listas constan de entre 10 y 12 pasos que se enumeran a continuación.

1. Concientización: Asegurarse que el personal de la compañía está al tanto de la nueva regulación y entiende sus implicancias e impacto

2. Consentimiento: La reglamentación es más exigente en cuanto al consentimiento de los individuos y por lo tanto se debe revisar y adecuar los procesos y documentos actuales sobre el tema asegurando un consentimiento explícito y activo. El lenguaje

debe ser más claro y transparente así como también el propósito de la recolección de datos.

3. Alcance internacional: La nueva ley no solo alcanza a organizaciones europeas sino que la reglamentación se aplica a todos los responsables y encargados del tratamiento de datos establecidos en la Unión Europea y a las organizaciones que ofrezcan servicios a ciudadanos de la Unión Europea [50]. A su vez se debe verificar que los procedimientos actuales cumplan con las condiciones impuestas para efectuar transferencias de datos fuera del territorio de la unión europea

4. Derechos de los individuos: Como ya se ha mencionado, GDPR brinda más derechos a los individuos, con lo cual se debe tener consideración en términos de “derecho al olvido”, “derecho al acceso a información personal”, “portabilidad”, “derecho a corregir información incorrecta” y ”decisiones automáticas basadas en creación de perfiles” entre las más relevantes.

5. Menores de edad: La organización debería cerciorarse que la información personal que recolecta no proviene de menores de edad y si es así correspondería conseguir la autorización de sus padres, tutor o encargado para poder operar con la misma

6. Procesamiento de datos: Quienes procesen datos a partir de ahora será responsables de que los métodos utilizados para efectuar su análisis sean compatibles con GDPR ya no podrán delegar la responsabilidad en quienes los contraten para efectuar el procesamiento

7. DPOs: Como ya hemos mencionado esta figura se incorpora al nuevo escenario que presenta la reglamentación obligando a las organizaciones a crear esta nueva figura en sus organigramas o bien contratar una consultora especialista y calificada cumpla este rol.

8. Notificaciones: A partir de la nueva reglamentación todos los incidentes de seguridad deberán ser reportados de inmediato (por lo menos dentro de las primeras 72 hs. de ocurrido el incidente). Estas notificaciones deben ser claras y detallar los procedimientos tomados en consecuencia para neutralizar su impacto. Así como también deberán alcanzar a quienes hayan sido damnificados.

9. Privacidad desde el diseño y por defecto: La nueva regulación establece que los procesos de tratamiento de los datos personales deben estar desde el principio alineados con GDPR y brindar la máxima protección de acuerdo a la tecnología vigente. Asimismo, se deben implementar mecanismos que permitan asegurar por defecto que solo la información personal necesaria es almacenada y utilizada respetando el tiempo de retención, y uso de la misma para los propósitos que fue recolectada. En particular se debe verificar que por defecto los datos personales no puedan ser accedidos sin intervención o previa autorización.

10. Sanciones: la organización debe ser consciente de las potenciales multas que se le aplicarán sin no cumple con la nueva regulación a partir de la fecha estipulada

Estos ítems son, a grandes rasgos, los cambios más relevantes y significativos de la nueva regulación y los que de seguro deberán ser atendidos por las organizaciones antes de Mayo 2018 para encontrarse totalmente alineados con la nueva ley GDPR

8. Big data bajo la lupa de GDPR

Luego de haber profundizado en diferentes aspectos de GDPR, una de las grandes incógnitas es como lograrán las nuevas tecnologías adaptarse a esta nueva reglamentación.

Sin duda Big data y “creación de perfiles” son técnicas en auge en la actualidad que se verán impactadas por las nuevas restricciones.

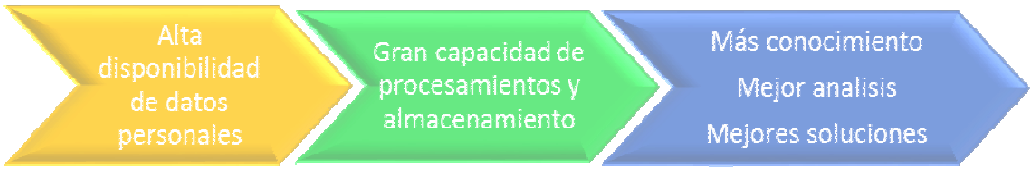
En términos generales podríamos definir “Big data” como la tendencia en el avance de la tecnología que ha abierto las puertas hacia un nuevo enfoque de entendimiento y toma de decisiones, la cual es utilizada para describir enormes cantidades de datos (estructurados, no estructurados y semi estructurados) que tomaría demasiado tiempo y sería muy costoso cargarlos a un base de datos relacional para su análisis.

De esta manera, el concepto de Big Data aplica para toda aquella información que no puede ser procesada o analizada utilizando procesos o herramientas tradicionales. [21]

Las organizaciones han atacado esta problemática desde diferentes ángulos, utilizando diferentes herramientas y tecnologías para lograr efectuar análisis de datos a gran escala con resultados que realmente agreguen valor y ayuden en la toma de decisiones. Dentro de todas las opciones vigentes la que actualmente tiene el liderazgo en términos de popularidad para analizar enormes cantidades de información es la plataforma de código abierto Hadoop.

Hadoop está inspirado en el proyecto de Google File System (GFS) y en el paradigma de programación MapReduce, el cual consiste en dividir en dos tareas (mapper – reducer) para manipular los datos distribuidos a nodos de un clúster logrando un alto paralelismo en el procesamiento. [22]

Big data facilita un análisis de información en tiempo real para usos comerciales y gubernamentales sin precedentes.



8.1. Alcance de GDPR

A partir de la nueva reglamentación, y a diferencia de su antecesora, la directiva 95/46/EC el alcance de la ley es más amplio ya que no solo se aplica a controladores localizados en la unión europea, sino que se incluyen controladores de datos y compañías fuera del territorio de la unión europea que procesen datos personales de residentes europeos.

Por su parte, el artículo 22 de GDPR introduce cambios como:

- Una definición explicita de “creación de perfiles”
- El consentimiento explícito como una nueva obligación para las actividades de “creación de perfiles”
- La prohibición de generar perfiles individuales basados en data sensible(a menos que exista un consentimiento explícito)
- Obligación de notificar a los sujetos de datos específicamente que se va a hacer con sus datos personales; desde donde se encontrarán sus datos hasta la lógica aplicarles (artículo 13[1]).

8.1.1 Creación de perfiles

La normativa GDPR define “creación de perfiles“ como “cualquier método automatizado de procesamiento de datos personales que

implique el uso de datos personales para evaluar aspecto personales relacionadas a la naturaleza de la persona, en particular para analizar o predecir aspectos concernientes al desempeño laboral, situación económica, estado de salud, preferencias personales, intereses, comportamiento, ubicación o movimientos"[1]

En definitiva, "creación de perfiles" es cualquier forma automatizada de procesamiento de datos personales que consiste en utilizar la información para evaluar determinados aspectos personales de un individuo, en particular para analizar o predecir aspectos relacionados a su desempeño laboral, su situación económica, salud, preferencias personales, intereses, comportamiento, ubicación y movimientos[1]

Esta nueva tecnología puede ser utilizada para automatizar decisiones respecto a los individuos en base a una fórmula o calculo previamente definido, por ejemplo se puede implementar un algoritmo que calcule la prima de seguro a ofrecer a sus clientes vía web en forma totalmente automatizada o un sistema automatizado de reclutamiento de personal.

Dados los riesgos en términos de privacidad de estas decisiones automatizadas, la reglamentación estipula que las mismas pueden ser implementadas pura y exclusivamente con el consentimiento explícito de los individuos alcanzados.

La política a su vez, establece que las compañías tienen la obligación de informar a las personas que sus datos serán utilizados para efectuar un análisis de este tipo (por ejemplo, creación de perfiles") y cuál será la lógica a utilizar sobre su información personal así como también sus consecuencias.

8.2. Retención y transparencia

Las organizaciones están obligadas a comunicar a los individuos los periodos de retención de su información personal para sus actividades de análisis y los usos que le darán a su información personal, tanto la lógica que se le aplicará como el lugar donde residirán los datos

8.3. Consentimiento

Como ya hemos mencionado, GDPR obliga a solicitar el consentimiento del individuo, el cual debe ser brindado libremente para los usos especificados e informados previamente. Sin embargo, resulta muy complicado identificar el propósito del procesamiento de la data personal para investigaciones y análisis al momento de la recolección de la información. Por eso, existe el riego que la persona niegue el consentimiento ya que la justificación o destino de los datos puede ser muy ambigua, amplia y poco clara.

8.4. Evaluación de impacto

Una evaluación de impacto es una herramienta sumamente importante para identificar y mitigar riegos de privacidad antes del procesamiento de la data. En particular en GDPR este análisis es un requisito más para el análisis con grandes volúmenes de datos personales. Por lo tanto comienzan a surgir esquemas de certificación para demostrar compatibilidad en materia de protección de grandes volúmenes de datos.

Para procedimientos como la “creación de perfiles” que utilizan datos sensibles y privados, la ley establece que se deberá llevar a cabo un análisis de impacto previo comienzo del procesamiento.

La integridad y calidad de los datos son esenciales para efectuar análisis de datos sobre Big Data. Si el estudio se efectúa sobre datos “sucios” o incompletos, las decisiones a tomar basadas en esta información serán erradas.

8.5. Minimización y calidad de la información

Grandes volúmenes de datos están disponibles en el mundo pero no todos son de buena calidad, por lo que GDPR propone restringir el almacenamiento solo a los datos indispensables para el análisis [24]

Figura 8 – Minimización y procesamiento de los datos personales

Por su parte, la nueva normativa promueve un cambio de paradigma en el cual el controlador de los datos debe adoptar ciertas medidas para asegurar y demostrar alineamiento con la misma (artículo 24)[3] así como también evaluar, analizar y minimizar los riesgos asociados al procesamiento.[24]

Otra alternativa de la minimización es la seudonimización, que consiste en excluir los datos denominativos del individuo –es decir aquéllos que lo pueden identificar de manera directa-, si es que potencialmente permiten, a través de la asociación con información adicional, determinar quién es el individuo.

Para esto se determina que la información adicional que permite efectuar la asociación debe encontrarse protegida para impedir la determinación de la persona afectada. Este tipo de metodología prevé una facilidad adicional en su tratamiento dentro de la normativa ya que disminuye los riesgos en caso de una filtración de información. A su vez, en los casos que no se disponga del consentimiento explícito del individuo, la seudonimizacion puede colaborar a que el mismo sea lícito con base legal en un fin de interés legítimo ya que es uno de los factores citados que ayuda a determinar la compatibilidad del tratamiento.

Sin embargo, si no es implementada debidamente, por el contrario, en vez de limitar el riesgo y considerarse una medida de seguridad, esta metodología puede tener consecuencias graves para las compañías en los casos en que haya una reversión no autorizada de la seudonimización. Por lo tanto, es una herramienta que, aportando

ventajas evidentes, debe ser cuidadosamente valorada para determinar su aplicabilidad. [23]

A simple vista, parece que la nueva reglamentación intenta restringir el uso de esta tecnología. Sin embargo, lo que esencialmente busca es la protección de los individuos y su información personal transformando la regulación en una inversión indispensable para ganar la confianza de los ciudadanos y que la misma sea un valor a buscar y desarrollar.

9. **Conclusiones**

La implementación de las políticas de privacidad es un tema complejo pero indispensable que nos afecta a todos. En particular GDPR representa un desafío importante para todo tipo de empresas y particulares ya que abarca aspectos nunca antes tomados en cuenta por una reglamentación de privacidad.

Uno de sus cambios claves, más fuertes y profundos, es el de las sanciones. Como se menciona en el desarrollo del trabajo, las sanciones son altas y pueden alcanzar sumas exorbitantes. Esto le da impulso y peso a la reglamentación y brinda una razón más para prestarle especial atención a las organizaciones alcanzadas por la misma

Además, como se ha explicado, la nueva política impone cambios organizacionales significativos; desde los procesos hasta nuevos roles, siendo el de mayor relevancia la nueva figura del DPO.

Esta nueva figura tomará un lugar crítico en la organización, su perfil será muy buscado y a la vez modelado en los próximos años. En la actualidad ya se han comenzado a crear carreras, certificaciones, y cursos de posgrados para poder acercar al profesional de Seguridad de la Información a una formación académica acorde a esta nueva necesidad y posición.

Sin embargo, los costos que conllevan la adaptación a esta medida (si bien existe un periodo para gestionar el cambio) son altos y las empresas recién empiezan a darse cuenta que deben hacer algo al respecto.

En particular GDPR presenta una serie de medidas necesarias pero innovadoras que expone los riesgos y debilidades de otros modelos utilizados en el mundo.

Tal como se ha analizado, el caso de Estados Unidos, si bien tiene similitudes, no se encuentra tan fuertemente impuesto como se propone en la reglamentación europea. Por su parte Canadá, se encuentra más cerca de GDPR pero no tiene el mismo alcance y peso.

Para el caso de nuestro país, las políticas de privacidad aún se encuentran en pleno desarrollo. Si bien la reglamentación actual se encuentra

desactualizada de acuerdo al avance de la tecnología, el panorama y los planes de una nueva ley de privacidad de datos personales en Argentina son prometedores y se encuentran muy avanzados. Con lo cual no sorprendería en el próximo año ver algún cambio o avance en este sentido.

Tecnologías vigentes y de vanguardia como computación en la nube o Big data deberán re adaptarse a la nueva realidad impuesta por esta nueva política que promete velar por los derechos a la privacidad de los individuos. Por supuesto que estos cambios llevarán tiempo y tendrán un costo asociado, pero a su vez brindarán cierto respaldo y un valor agregado a la sociedad: la garantía de que su privacidad se encuentra protegida.

En mi opinión, la nueva reglamentación es un cambio necesario que viene para quedarse y es un ejemplo a seguir para otros países y regiones. Los individuos se sentirán más seguros en tanto se mantenga actualizada la ley de acuerdo a la evolución y avance de la tecnología. A su vez, la misma sienta las bases para una reglamentación básica global para lo cual deberán alinearse los países y ponerse de acuerdo en aspectos básicos, pero al mismo tiempo garantizará la protección de la privacidad de cualquier persona en el ciberespacio a nivel global.

Puede que la UE tenga que extender el plazo para la implementación de las políticas ya que las empresas recién ahora, a pocos meses de finalizar el plazo máximo, están incluyendo en sus planes la adaptación a GDPR, pero vale la pena. Será cuestión de tiempo para ver los frutos de esta nueva reglamentación y observar cómo otros toman el ejemplo y adaptan las suyas a la nueva realidad que estamos viviendo.

Bibliografía

[1] General Data Protection Regulation, sitio oficial de la política, http://www.Eugdpr.org, 2017 (fecha de consulta 20/4/2017)

[2] Versión final de la regulación, http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf , versión 6, Abril 2016 (fecha de consulta 20/4/2017)

[3] The Organization for Economic Co-Operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html , Enero, 1999 (fecha de consulta 20/4/2017)

[4] Sitio oficial Eset España, http://gdpr.eset.es/, 2017 (fecha de consulta 20/4/2017)

[5] Infografía GDPR, Consultora PSN Sercon, https://psnsercon.com/blog/wp-content/uploads/2016/07/infografia-reglamento.png, 2017 (fecha de consulta 20/4/2017)

[6] Sitio oficial del Parlamento Europeo, http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuId=FTU_5.12.8.html , 2017 (fecha de consulta 20/4/2017)

[7] Directiva 95/ 46/ EC http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046, 2017 (fecha de consulta 20/4/2017)

[8] Ateneu Privacy Consulting, http://ateneu.eu/es/publicacion-oficial-reglamento-europeo-proteccion-datos-c223, 2017 (fecha de consulta 20/4/2017)

[9] Welivesecurity, https://www.welivesecurity.com/la-es/2017/02/10/gdpr-buena-o-mala-noticia, 2017 (fecha de consulta 20/4/2017)

[10] marketing4ecommerce, Patricia Villanueva, https://marketing4ecommerce.net/nueva-normativa-proteccion-datos-ue-gdpr/ , Mayo 2017 (fecha de consulta 20/4/2017)

[11] Veritas Technologies, https://www.veritas.com/content/dam/Veritas/docs/reports/gdpr-report-en.pdf, 2017 (fecha de consulta 20/4/2017)

[12] Alberto Iglesias Fraga, http://www.ticbeat.com/seguridad/el-70-de-las-empresas-europeas-no-cumplira-con-el-gdpr-a-tiempo/, 2017 (fecha de consulta 20/4/2017)
[13] Ateneu Privacy Consulting, Josep Aragonés Salvat, http://ateneu.eu/es/autoridad-control-gdpr-c257 , 2016 (fecha de consulta 20/4/2017)
[14] Ateneu Privacy Consulting, Josep Aragonés Salvat, http://ateneu.eu/es/delegado-proteccion-datos-gdpr-c254, 2017 (fecha de consulta 20/4/2017)
[15] Ateneu Privacy Consulting, Josep Aragonés Salvat, http://ateneu.eu/es/aplicacion-gdpr-responsabilidad-tratamiento-c265, 2017 (fecha de consulta 20/4/2017)
[16] Ateneu Privacy Consulting, Josep Aragonés Salva, http://ateneu.eu/es/aplicacion-gdpr-derechos-interesado-c274 , 2017 (fecha de consulta 20/4/2017)
[17] Ateneu Privacy Consulting, Josep Aragonés Salva, http://ateneu.eu/es/aplicacion-gdpr-garantias-cumplimiento-documentacion-c276, 2017 (fecha de consulta 20/4/2017)
[18] http://pwcspain.typepad.com/blog_nuevas_tecnologias/2015/01/protección-de-datos-desde-el-diseño.html, 2015 (fecha de consulta 20/4/2017)
[19] Ateneu Privacy Consulting, Josep Aragonés Salva, http://ateneu.eu/constructor/download.php?cfa=ac9d7a89421b3ca54f713630271e0d5c , 2017 (fecha de consulta 20/4/2017)
[20] Gartner https://www.gartner.com/doc/3463517/focus-highpriority-changes-tackle-eu, 2016 (fecha de consulta 20/4/2017)
[21] IBM, https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/, 2017 (fecha de consulta 20/4/2017)
[22] Apache Hadoop en http://hadoop.apache.org/ (fecha de consulta 20/4/2017)
[23] PWC España, http://periscopiofiscalylegal.pwc.es/reglamento-europeo-de-proteccion-de-datos-la-seudonimizacion, 2017 (fecha de consulta 20/4/2017)

[24] Big Data and the New EU Data Protection Regulation (GDPR), http://www.ema.europa.eu/docs/en_GB/document_library/Presentation/2017/01/WC500219338.pdf, Noviembre 2016 (fecha de consulta 20/4/2017)
[25] Comparativa de la Protección de Datos en Europa y en Estados Unidos, Eric Plaza, http:// www.eljurista.eu/2015/04/26/comparativa-de-la-proteccion-de-datos-en-europa-y-en-estados-unidos/ , 2016 (fecha de consulta 30/07/2017)
[26] Data Protection Laws of the World, https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all, 2017 (fecha de consulta 30/07/2017)

[27] Datos personales en EEUU tras el escudo de privacidad: Privacy Shield, https://www.hiberus.com/legaltech/blog/datos-personales-eeuu-privacidad-privacy-shield/ , 2016 (fecha de consulta 30/07/2017)
[28] Computación en la nube http://cibernat.com/articulos/computacion-en-la-nube , 2009 (fecha de consulta 30/07/2017)
[29] IAPP Canada, Privacy Symposium, https://www.slideshare.net/constantk/impact-of-gdpr-on-canada-may-2016-presented -at-iapp-canada-symposium, 2016 (fecha de consulta 30/07/2017)
[30] You've migrated to the cloud – what does GDPR mean for your business?, https://cloudcomputing-news.net/news/2017/mar/16/youve-migrated-cloud-what-does-gdpr-mean-your-business/, 2017 (fecha de consulta 30/07/2017)
[31] The GDPR's impact on the cloud service provider as a processor, Mark Webber, http://www.fieldfisher.com/media/3993765/the-gdprs-impact-on-the-cloud-service-provider-as-a-processor-mark-webber-privacy-data-protection.pdf, 2017 (fecha de consulta 30/07/2017)
[32] La TI híbrida, una ayuda necesaria para cumplir con el GDPR, http://hybrid-it.reimagineit.es/noticias/2017/05/la-ti-hibrida-una-ayuda-necesaria-para-cumplir-con-el-gdpr, 2017 (fecha de consulta 30/07/2017)
[33] How will the GDPR affect security in cloud computing? , http://www.bluesource.net/2017/05/12/how-will-the-gdpr-affect-security-in-cloud-computing/, 2017 (fecha de consulta 30/07/2017)

[34] Privacy and the EU GDPR Research Report 2017,

http://go.trustarc.com/a0300G08DL0l00rZnLfoJQy , 2017(fecha de consulta 09/08/2017)

[35] Mencionado por J. R. Helmig, experto en crímenes financieros y ex miembro del departamento de defensa de los EEUU, en su disertación “AML y Crímenes Financieros” en la empresa SAS, https://www.sas.com/es_ar/events/17q3/aml-10ago-2017/presenters.html, 10/08/2017

[36] DIRECTIVA (UE) 2016/680, http://www.boe.es/doue/2016/119/L00089-00131.pdf, 4 de mayo de 2016

[37] ¿Qué es una nube híbrida? https://azure.microsoft.com/es-es/overview/what-is-hybrid-cloud-computing/?cdn=disable , 2017

[38] Mastering Article 30 Compliance: Conducting, Maintaining & Reporting on Your Data Inventory, https://info.trustarc.com/on_demand_webinar.html?asset=7VGPPFAR-680&aliId=39796134#slides, 16 de agosto de 2017

[39] Hacia la seguridad de los datos después del reglamento europeo, José Luis Rivas López, Victor Salgado Seguín, http://www.rediris.es/jt/jt2016/ponencias/?id=jt2016-jt-sesi_par_1b-a11b1c1.pdf, 28 de septiembre de 2016

[40] Study: At least 28,000 DPOs needed to meet GDPR requirements https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/ , 19 de abril de 2016

[41] GDPR Matchup Argentinas Draft dat Protection, Pablo A. Palazzi, Andres Chomczyk, https://iapp.org/news/a/gdpr-matchup-argentinas-draft-data-protection-act/, 2017 (fecha de consulta 24/08/2017)

[42] CommuniGator: Your GDPR Compliance Checklist, http://mkt.gatorresources.co.uk/gatormaillz/lz.aspx?p1=05799906S6091&CC=&w=5561&cID=0&cValue=1 , 2017 (fecha de consulta 24/08/2017)

[43] CHECKLIST FOR TASKS NEEDED IN ORDER TO COMPLY WITH GDPR, https://gowlingwlg.com/GowlingWLG/media/UK/pdf/170630-gdpr-checklist-for-compliance.pdf, 2017 (fecha de consulta 24/08/2017)

[44] The GDPR at a glance, and a “to do” list to help you prepare for it, http://www.linklaters.com/pdfs/mkt/london/General_Data%20Protection_RegulationGDPR_Brochure_WEB_FINAL_Spreads4.pdf, 2017 (fecha de consulta 24/08/2017)

[45] GDPR Compliance Checklist, http://www.globalprivacyblog.com/files/2017/05/GDPR-Compliance-Checklist-003.pdf, 2017 (fecha de consulta 24/08/2017)

[46] Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now, https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf , 2017 (fecha de consulta 24/08/2017)

[47] GDPR checklist, Norton Rose Fulbright, http://www.nortonrosefulbright.com/files/gdpr-checklist-139465.pdf, 2017 (fecha de consulta 24/08/2017)

[48] GDPR Checklist, http://www.tp.co.uk/media/184106/gdpr-checklist.pdf , 2017 (fecha de consulta 24/08/2017)

[49] GENERAL DATA PROTECTION REGULATION (GDPR) 12 STEP CHECKLIST, https://www.eiseverywhere.com/file_uploads/3afa71b5cde79d4fd57e695b182b577d_REPLACE--HANDOUTImplicationsofNewDataProtectionandPrivacyRegulationsforTestSponsorsProvidersandUsersintheEU.pdf, 2017 (fecha de consulta 24/08/2017)

[50] El Derecho al Olvido y la Portabilidad de los Datos, las obligaciones más complejas para las empresas, http://www.ey.com/es/es/newsroom/news-releases/news-ey-nuevo-reglamento-general-de-proteccion-de-datos (fecha de consulta 24/09/2017)

Anexo

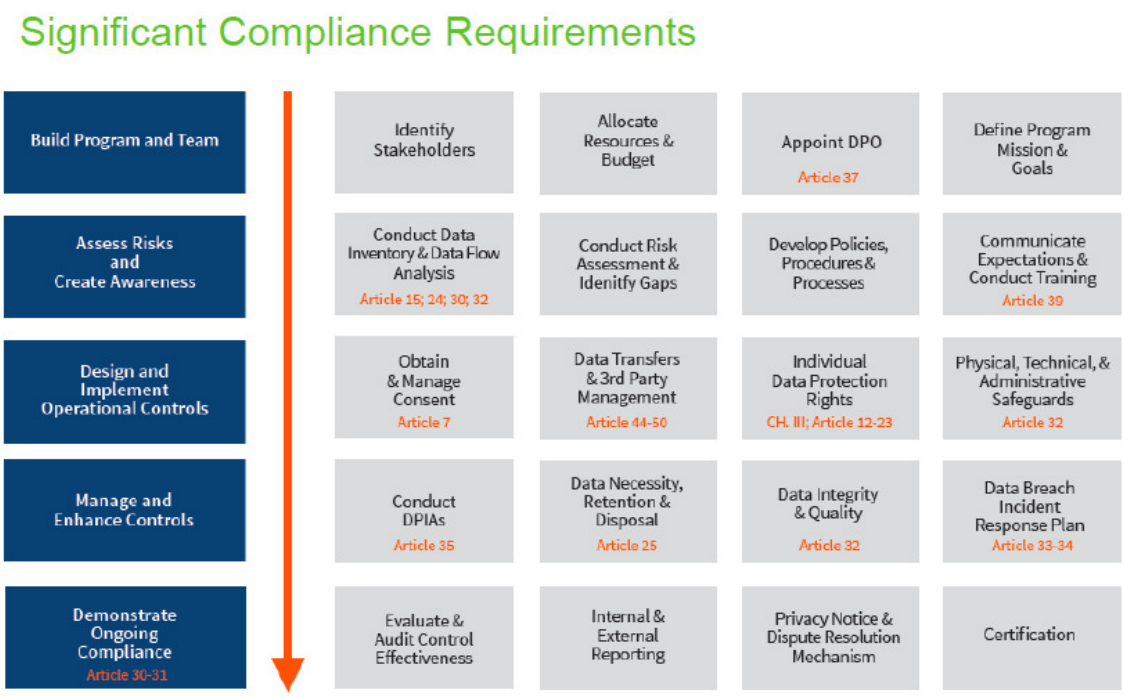


Figura 9 Requerimientos principales de GDPR [38]

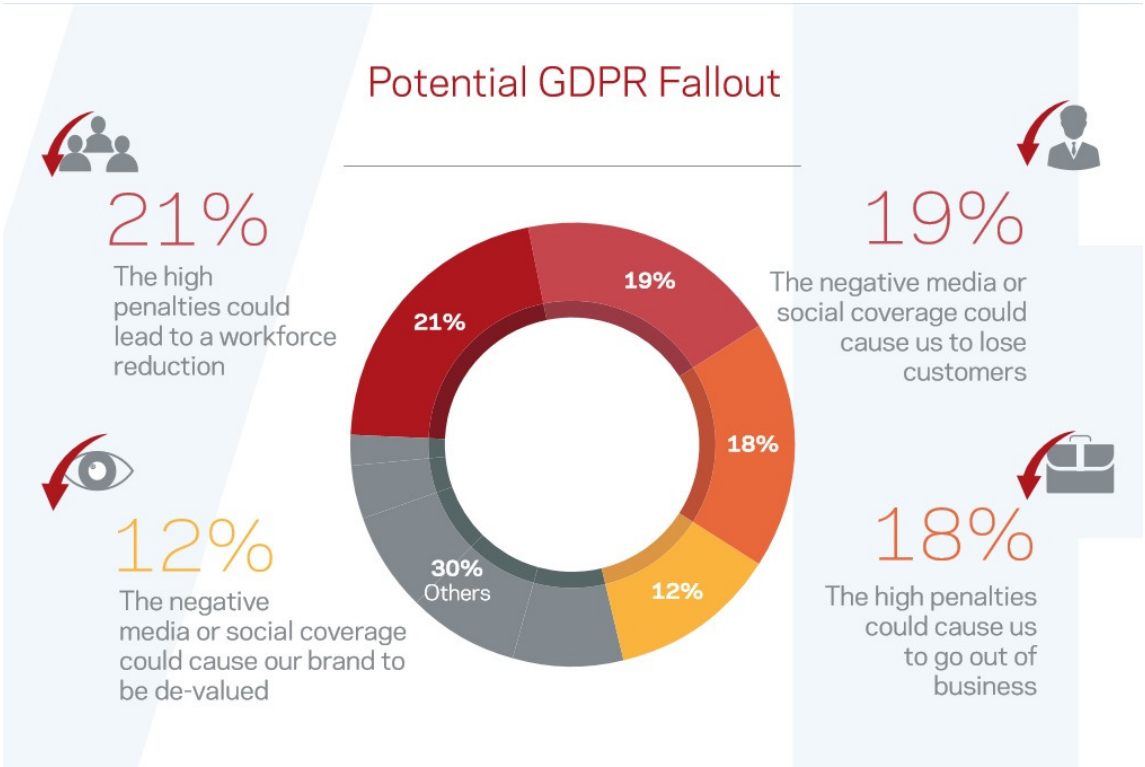


Figura 10 - Veritas Report [12]

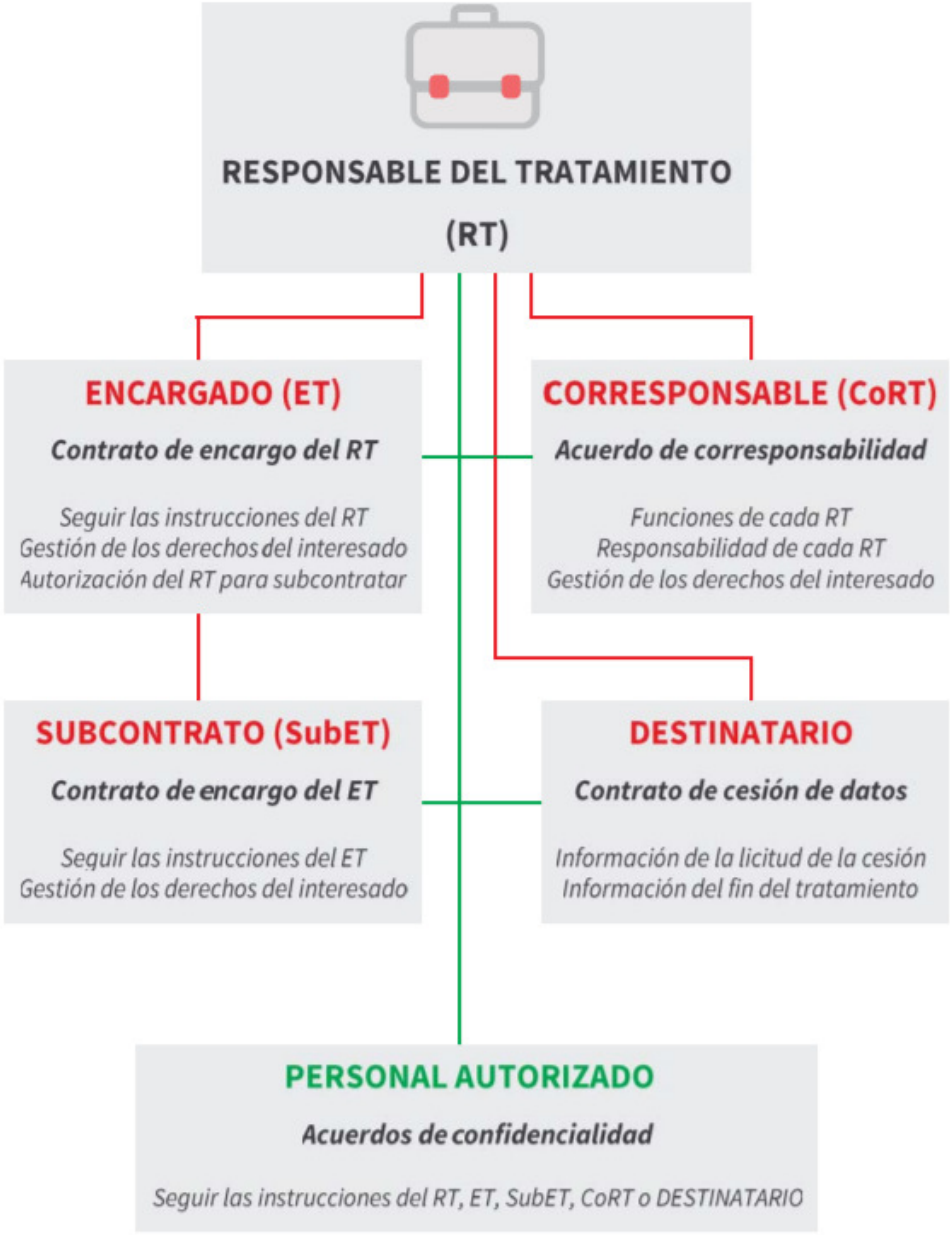


Figura 11- Intervinientes del tratamiento de los datos [19]

Figura 12 - Registro de actividades del responsable del tratamiento de los datos y el encargado del tratamiento de los datos [19]

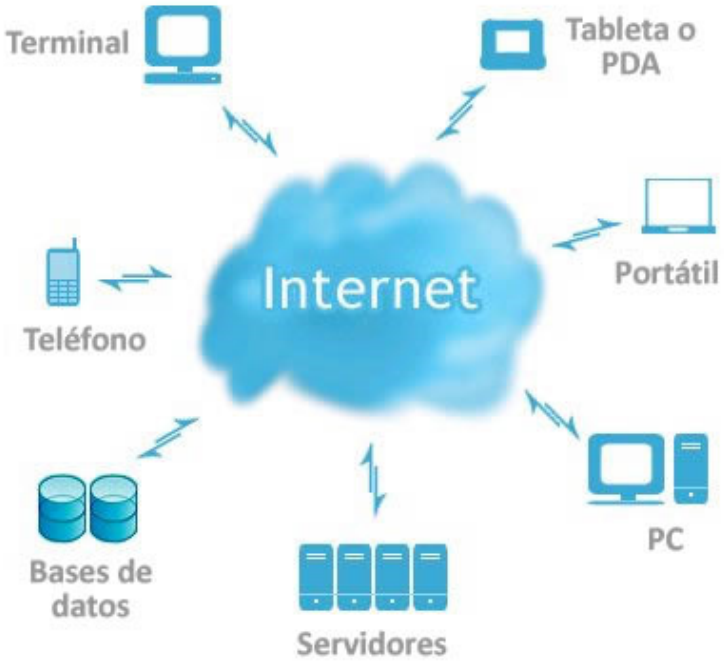


Figura 13- Diagrama de arquitectura de computación en la nube [28]

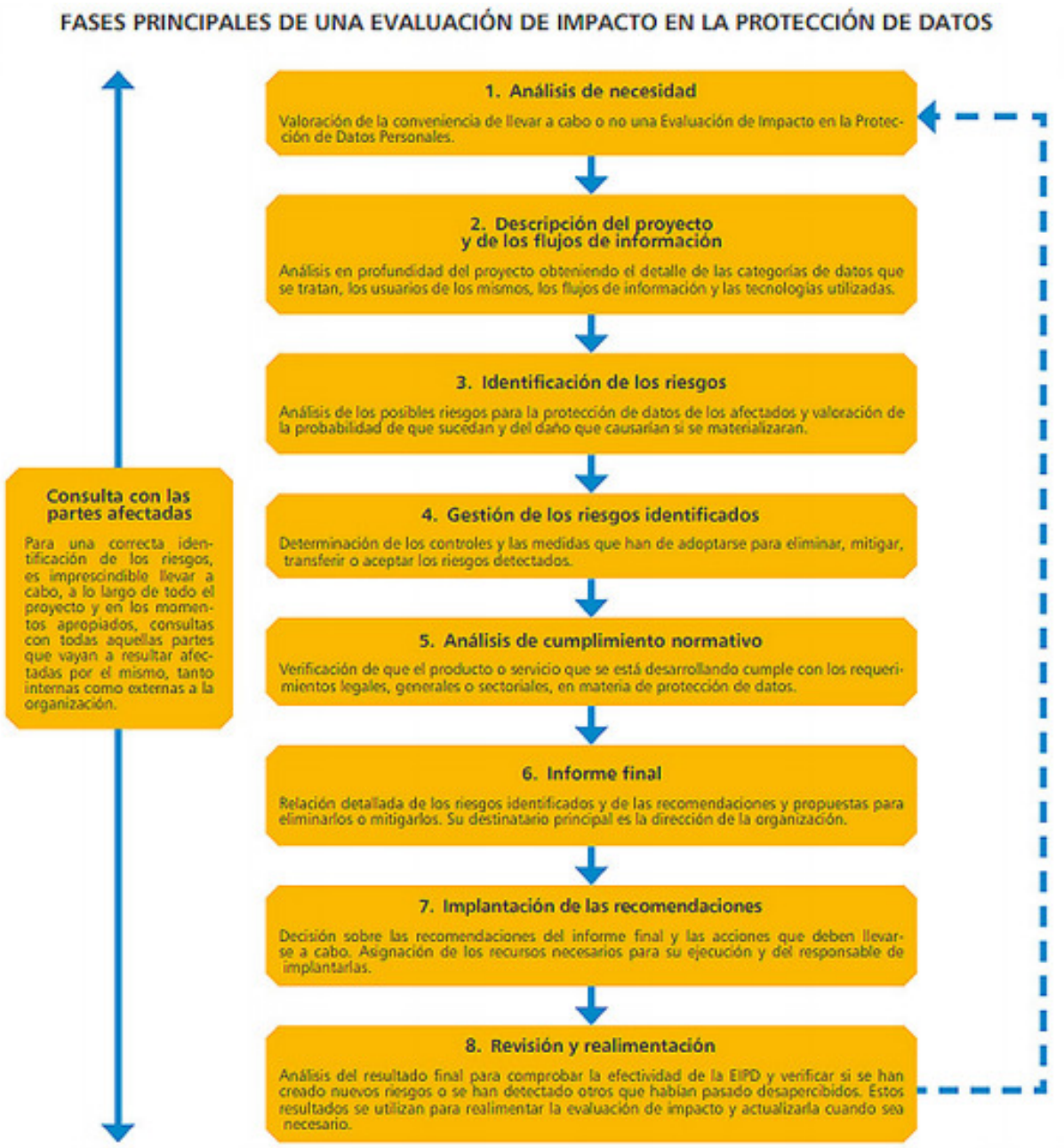


Figura 14- Fases de la evaluación de impacto [39]