PUBLIC

ROQUETTE
Offering the best of nature™

Privacy & Data Protection

CÓMO NOS COMPROMETEMOS CADA DÍA CON LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS

Privacidad y Protección de Datos

Guía de Buena Conducta

GRUPO ROQUETTE

Departamento jurídico y de conformidad

Principales retos de conformidad para Roquette

Bajo la égida de la Dirección general, el ámbito de la conformidad y su gestión dentro de Roquette han sido confiados al Departamento Jurídico y de Conformidad del Grupo, que se ha dotado de una Compliance Office.

La Compliance Office está a cargo del Código de conducta, de su actualización y de su aplicación.

Abarca las tres principales áreas siguientes:

- Seguridad financiera,
- Ética profesional y
- Privacidad y protección de datos.

Por lo tanto, se ha desarrollado un programa de conformidad que está evolucionando para garantizar que nuestra empresa sea legalmente y financieramente irreprochable.

¿Cuál es el papel de la conformidad?

El papel de la conformidad consiste en inculcar los **valores éticos** e implementar medidas de acuerdo con los **requisitos legales, las normas** y las **buenas prácticas.**

Nuestro Programa facilita la aplicación de los procedimientos que garantizan la conformidad con las reglas aplicables a Roquette.

Nuestros cuatro valores –**autenticidad, excelencia, orientación al futuro, bienestar**– constituyen la sólida base sobre la que actuamos **cada día**.

Hay que tener en cuenta que, hoy en día, una empresa sostenible es una empresa ética.
Y que la empresa del mañana es la empresa transparente.

Pensar global
Actuar local

Editorial

Los principios de la Privacidad y la protección de datos forman parte de las normas establecidas en el Código de conducta.

Todos los empleados, así como los terceros con los que Roquette tenga una relación, tienen derecho a la privacidad. Por esta razón, Roquette se ha comprometido a proteger sus datos personales.

Los datos personales son información que permite identificar directa o indirectamente a una persona física (nombre, fecha de nacimiento, número de seguridad social, fotografía, dirección de correo electrónico, ID del ordenador, etc.).

La protección de los datos personales es un derecho fundamental que garantiza la privacidad

La protección de los datos personales garantiza a cada individuo el derecho a controlar la recogida, tratamiento, uso y difusión de estos datos.

Los datos personales se deben utilizar de una forma justa para un fin específico, explícito y legítimo y únicamente se deben conservar durante el periodo necesario para realizar el tratamiento.

En Europa, el tratamiento de los datos personales está regulado por el Reglamento general de protección de datos (RGPD), que entró en vigor el 25 de mayo de 2018.

Puesto que la legislación en materia de datos personales y privacidad varía de un país a otro, y dado que Roquette está presente en todo el mundo, el Grupo ha adoptado una Política del Grupo relativa a la protección de los datos personales. Esta política se aplica a todos los empleados del Grupo en todo el mundo.

Esta Guía explica la Buena conducta que debemos adoptar en nuestras actividades diarias para cumplir los Principios de la protección de datos personales y los requisitos de nuestra Política.

Jennifer GODIN, Responsable de protección de datos

Déléguée à la protection des données

Índice de contenidos

Departamento jurídico y de conformidad 3
Editorial de la Responsable de protección de datos 4

Objetivo 6
Descripción 7
Responsabilidades 8
Plantear preguntas o inquietudes 9
Cumplimiento de las leyes y los reglamentos 10
Principios de la protección de datos 12
Riesgo de privacidad 14
Riesgos en caso de incumplimiento 16

Nuestras normas en nuestras relaciones con los Titulares de los datos > p. 19

- Cultura de la privacidad 20
- Tratamiento de los datos 22
- Derechos de los titulares de los datos 24
- Aviso de privacidad 26
- Minimización de datos 28
- Seguridad de los datos 30
- Clasificación de la información personal 32
- Conservación de datos 34

Nuestras normas en nuestra relación con los Afiliados y Subcontratistas > p. 37

- Cualificación de responsable y encargado 38
- Cláusulas de protección de datos 40
- Acuerdo de transferencia de datos 42

Nuestras normas en nuestra relación con nuestra Red y las Autoridades de supervisión > p. 45

- Responsable de protección de datos 46
- Red de protección de datos y partes interesadas 48
- Autoridades de supervisión 50
- Gobernanza 52
- Responsabilidad 54
- Documentación 56
- Evaluación de impacto en la privacidad 58
- Privacidad desde el diseño y por defecto 60
- Notificación de la violación de datos 62
- Revisión y supervisión 64

Documentos de referencia 66
Bibliografía 67
Fuentes 68

Objetivo

¿Qué es la política de privacidad y protección de datos?

El Grupo Roquette ha establecido una Política de Privacidad y de Protección de Datos (la "Política") para abordar mejor los problemas de Privacidad y Protección de Datos de acuerdo con su imagen, sus intereses y las legislaciones y regulaciones aplicables en materia de protección de datos.

Esta Política define los principios y requisitos para la protección de la información personal e indica las reglas que deben respetar todos los empleados, directivos, directores y terceros que actúen para Roquette en términos de Privacidad y Protección de Datos.

Los principios y reglas de esta Política de protección de datos personales se detallan en una plataforma documental con tres niveles:

- Compromiso de la dirección: Código de conducta.
- Reglas internas Manual y directrices de protección de datos personales en Q-Docs.
- Documentación del Sistema de gestión de la protección de datos (SGPD): Procedimientos, orientaciones, metodologías, aprendizaje, etc.

Toda la documentación cumple los requisitos legales y reglamentarios relativos a la protección de datos.

¿Qué es la Guía de buena conducta en privacidad y protección de datos?

La Guía de privacidad y protección de datos (la "Guía") puede ayudarnos a implementar y cumplir con nuestra política de privacidad y protección de datos.

Esta presenta, de manera simplificada, las reglas y mejores prácticas que cumplen con las directivas de nuestro Grupo y los requisitos de las leyes y reglamentaciones aplicables a nuestra empresa en términos de protección de datos.

Se divide en temas inspirados en el Código de conducta, de los cuales la "Privacidad y protección de datos" es uno de los temas de la conformidad.

Descripción

¿A quién se aplica la Guía de buena conducta en privacidad y protección de datos?

La Política y la Guía son una base común para todas las entidades de todo el mundo. Se aplican a:

- Todos los empleados, consejeros y directivos (en adelante, los «Empleados»)
- Todos los terceros que actúen en nombre de Roquette, como:
  - Contratistas, incluidos los consultores, los autónomos y el personal temporal
  - Becarios
  - Personal desplazado de una entidad que no pertenezca a Roquette
  - Trabajadores eventuales
  - Otros representantes
  - Todo tercero empleado o pagado por Roquette.

¿Dónde podemos encontrar la Guía de buena conducta en privacidad y protección de datos?

Todos los empleados y terceros que actúen en nombre de Roquette deben entender y respetar los principios de Privacidad y protección de datos contenidos en nuestra Documentación y, más particularmente, en esta Guía.

Tiene la Guía a su alcance en el Portal ONE:

Funciones globales > Protección de datos > Guía de buena conducta.

Esta Guía se transmite como parte de una acción de comunicación específica, acompañada de un conjunto de herramientas con cursos de e-learning sobre los Principios de la Privacidad y la Protección de Datos (definidos por las normas internacionales y los requisitos específicos del RGPD).

Este curso de formación está incluido en el Programa de incorporación de la protección de datos.

Responsabilidades

¿Quién es responsable de la aplicación de los Principios operativos?

La privacidad de los datos es relevante para –y la responsabilidad de todas y cada una de las personas de nuestra empresa.

Todos tenemos la responsabilidad de respetar los Principios operativos descritos en la documentación del SGPD proporcionada por el Equipo de la Compliance Office y la Red de protección de datos. Esta Guía respalda su aplicación y aumenta nuestro nivel de conformidad.

¿Cómo podemos asegurarnos de que hemos adoptado la decisión correcta?

La Guía se ha diseñado para ayudarnos a tratar la mayoría de las situaciones de nuestra vida laboral que puedan plantear cuestiones relativas a la privacidad. No obstante, no puede prever todas las situaciones a las que nos podemos enfrentar en el ejercicio de nuestras actividades profesionales.

Si tenemos alguna duda, en cualquier momento, sobre la conducta que debemos adoptar, debemos plantearnos las siguientes preguntas:

- ¿Cumple esto la ley?
- ¿Repercute esto positivamente en mí y en la empresa?
- ¿Le hablaría a un amigo, familiar o compañero sobre esto?
- ¿Me sentiría cómodo si esto se hiciera público?

Si la respuesta a alguna de estas preguntas es «No», no deberíamos seguir adelante. Si tenemos dudas, deberíamos hablar con el Responsable de protección de datos del Grupo o con la persona de contacto correspondiente (véase la información de contacto en el apartado «Plantear preguntas o inquietudes»).

¿Qué sucede si no cumplimos los Principios de privacidad y protección de datos?

El hecho de no respetar los Principios puede tener una repercusión negativa para la empresa. Las consecuencias pueden ser muy graves, tanto para la empresa como para las personas implicadas (sanciones disciplinarias, multa, encarcelamiento, daños a la reputación, etc.).

Todas las denuncias de violaciones presuntas o reales de los Principios se tomarán muy en serio. Iniciaremos una investigación inmediatamente, de manera justa y de conformidad con los requisitos legales.

Dependiendo de la naturaleza de la violación de datos, se pueden imponer medidas disciplinarias, de acuerdo con las leyes locales y los reglamentos de la empresa.

Todos los empleados deben cooperar plenamente en las investigaciones. Roquette protegerá la confidencialidad de las personas implicadas.

Plantear preguntas o inquietudes

Se anima a los empleados, a los terceros que actúen en nombre de Roquette y a las demás partes interesadas a que planteen preguntas o inquietudes que ayudarán a Roquette a prevenir y reducir los daños a la empresa.

¿Qué tipo de cuestiones pueden plantearse?

Se puede plantear cualquier pregunta y cualquier violación real o potencial de los Principios de Privacidad y protección de datos, los reglamentos de la empresa o la legislación aplicable.

¿Con quién debemos ponernos en contacto?

En caso de Violación de datos, póngase en contacto con el Responsable de la Protección de Datos de Roquette dpo@Roquette.com y/o notificar un incidente mediante nuestro formulario web "Privacy Alert".

Si necesita notificar una posible infracción de la normativa, puede ponerse en contacto con su interlocutor habitual o notificar un problema a través del dispositivo Speakup©. Todas las alertas recibidas a través de este dispositivo se tratan de forma confidencial, respetando las leyes y normativas pertinentes.

SpeakUp®

Roquette no tolerará ningún tipo de represalia contra ningún empleado o tercero que denuncie, de buena fe, un incumplimiento real o potencial de los Principios de la protección de datos ni de las leyes aplicables.

Por lo tanto, si el emisor/a de una alerta profesional debe identificarse, su identidad debe ser procesada de manera confidencial por la organización, a fin de evitar el riesgo de represalias, discriminación o medidas disciplinarias contra él / ella por haber denunciado hechos.

Cumplimiento de las leyes y los reglamentos

Se espera que todos y cada uno de nosotros, en cada entidad del Grupo, cumplamos las leyes y reglamentos vigentes relativos a la Protección de datos.

En los casos en los que los reglamentos locales sean más estrictos que nuestra Política y nuestra Guía, prevalecerán los primeros.

En caso contrario (ausencia de legislación local o legislación menos restrictiva), nuestras buenas prácticas internas prevalecerán en la medida en que la ley lo permita.

Consideramos que:

- Debemos aplicar lo más rápido posible todos los nuevos reglamentos locales aplicables.
- Todos debemos ser conscientes de que el incumplimiento de las leyes y reglamentos puede estar sujeto a sanciones civiles y/o penales, tanto para la persona involucrada como para la empresa.
- La protección de los individuos en relación con el tratamiento de los datos personales es un derecho fundamental.
- Los principios y las normas sobre la protección de las personas físicas con respecto al tratamiento de sus datos personales deben, independientemente de su nacionalidad o residencia, respetar sus derechos y libertades fundamentales, en particular su derecho a la protección de datos personales.
- El derecho a la protección de datos personales no es un derecho absoluto; debe considerarse en relación con su función en la sociedad y equilibrarse con otros derechos fundamentales, de conformidad con el principio de proporcionalidad.

¿Qué país ha adoptado una legislación de protección de datos específica o tiene una Autoridad de Protección de Datos?

Para obtener una descripción general, consulte este mapa: https://www.cnil.fr/en/data-protection-around-the-world.

Nuestras responsabilidades:

- En todas las circunstancias, debemos cumplir todas las leyes y reglamentos relativos a la Protección de datos en los países de los titulares de los datos y todas las normas vigentes en cada uno de los centros de la empresa.

- En el marco de nuestras actividades profesionales, debemos informar de cualquier comportamiento que consideremos que va en contra de las leyes y regulaciones aplicables con respecto a la Protección de datos (por ejemplo: el RGPD) a nuestro Responsable de la Protección de datos en dpo@Roquette.com y el dispositivo de alerta confidencial Roquette: Speakup©.

- Debemos establecer medidas de protección de los datos personales que sean apropiadas y proporcionales al contexto, a la vez que facilitamos el cumplimiento de otras leyes y reglamentos. Por el contrario, nuestras acciones para cumplir con las leyes y regulaciones aplicables al Grupo deben cumplir con las reglas y buenas prácticas para la protección de datos personales (por ejemplo: en el programa de cumplimiento de lucha contra el soborno y la corrupción, debemos garantizar la protección del denunciante a través de medidas de confidencialidad y protección de sus datos personales).

¿Está usted sujeto al Reglamento General de Protección de Datos (RGPD)?

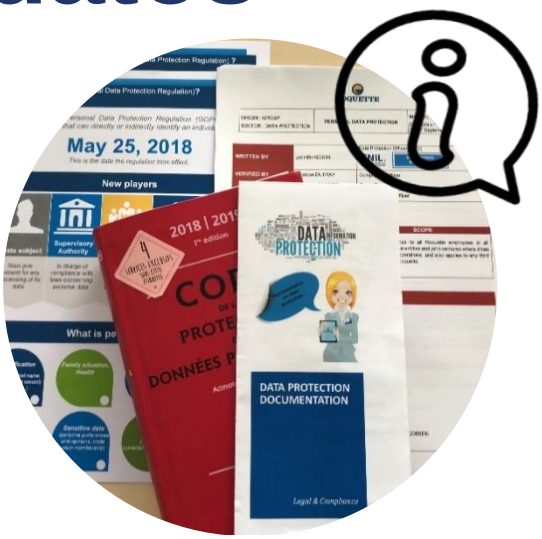
Usted entra en el alcance del RGPD como **responsable** (1) o **encargado** (2):

- si está establecido en la UE o;
- cuando no está establecido en la UE, si: sus "actividades de tratamiento están relacionadas con
  - la oferta de bienes o servicios a los titulares de los datos en la UE;
  - o la supervisión de su comportamiento en la medida en que su comportamiento tenga lugar dentro de la UE".

Texto oficial: Artículo 3 del RGPD sobre el alcance territorial

(1) y(2): Véanse las definiciones en la página 38.

Principios de la Protección de datos



Los datos personales deben ser:

- seguros.
- exactos y actualizados.
- tratados de manera justa y lícita.
- tratados con propósitos limitados.
- adecuados, pertinentes y no excesivos.
- conservados durante un periodo de tiempo limitado y determinado.
- tratados de acuerdo con los derechos de los titulares de los datos.
- protegidos con medidas legales adecuadas si se transfieren a otros países.

Sus derechos:

De acuerdo con la legislación y las reglamentaciones aplicables, tiene derecho a acceder, rectificar y oponerse al tratamiento de sus datos por razones legítimas, así como el derecho a borrar por razones legítimas, el derecho a la portabilidad de los datos y el derecho a limitar el tratamiento de sus datos.

Para ejercer estos derechos, complete el formulario disponible en: Roquette.com/Data Protection/Privacy Rights.

Para toda petición, contacte con el **Responsable de protección de datos** (dpo@Roquette.com).

Nuestras responsabilidades:

Debemos:

- Cumplir la legislación local y las reglas de la Política del Grupo sobre Protección de datos personales.
- Notificar al Responsable de la protección de datos cualquier nuevo tratamiento o cambio.
- No recopilar, usar, divulgar o almacenar datos de carácter personal a menos que sea para fines específicos, legítimos y necesarios.
- Asegurarse de que las personas hayan sido informadas de que se están recopilando sus datos.
- Proteger estos datos durante su recopilación, tratamiento, uso, comunicación, almacenamiento o transferencia.
- Garantizar la seguridad y la confidencialidad de los datos tratados.
- Conservar los datos solo durante el tiempo necesario para su tratamiento y cumplir las leyes aplicables.
- Ponerse en contacto con el Responsable de la protección de datos en caso de incidente de seguridad que afecte a los datos personales.

Formamos a nuestros empleados y mejoramos nuestros procesos internos.

Riesgo de privacidad

¿Qué es un riesgo de privacidad?

Un riesgo es un escenario hipotético que describe un evento temido y todas las amenazas que permitirían que esto ocurriera. Más específicamente, describe:

- cómo las fuentes de riesgo (por ejemplo, un empleado sobornado por un competidor)
- podrían aprovechar las vulnerabilidades de los activos de soporte (por ejemplo: el sistema de gestión de archivos que permite la manipulación de datos)
- en un contexto de amenazas (por ejemplo, mal uso al enviar correos electrónicos)
- y permitir que se produzcan los eventos temidos (por ejemplo: acceso ilícito a los datos personales)
- sobre los datos personales (por ejemplo: archivo del cliente)
- generando así impactos en la privacidad de los titulares de los datos (por ejemplo: solicitudes no deseadas, sentimientos de invasión de la privacidad, problemas personales o profesionales).

Efecto de la incertidumbre en la privacidad

La gravedad representa la magnitud de un riesgo. Se estima principalmente en términos del alcance de los posibles impactos (**físicos, materiales, morales**) en los titulares de los datos, teniendo en cuenta los controles existentes, planificados o adicionales.

Ejemplo:

El riesgo más importante que presenta el sistema de alerta profesional para el denunciante: el riesgo de represalias, discriminación o medidas disciplinarias contra él / ella por haber denunciado los hechos.

Consideramos que:

Los derechos de las personas se aplican en su totalidad, independientemente del nivel de riesgo en el tratamiento.

Sin embargo, se nos pedirá que modulemos nuestro cumplimiento de protección de datos de acuerdo con el nivel de riesgo que nuestras operaciones de tratamiento de los datos personales representan para los derechos y libertades fundamentales de las personas.

El RGPD da un mayor impulso a esta práctica. Por consiguiente, las operaciones de tratamiento que plantean menos riesgos para los derechos y libertades fundamentales de las personas generalmente pueden resultar en menos obligaciones de cumplimiento, mientras que las operaciones de tratamiento de "alto riesgo" plantearán obligaciones de cumplimiento adicionales, como la Evaluación del impacto en la protección de datos (DPIA)(1).

Nuestras responsabilidades:

La evaluación de los riesgos es fundamental. Según el RGPD, la consideración del riesgo subyace a la responsabilidad de la empresa y a todo el tratamiento de los datos.

Tenemos que realizar evaluaciones de los riesgos en el marco de las DPIA para el tratamiento de alto riesgo, así como en relación con muchos otros requisitos del RGPD, incluida la Seguridad de los datos, las notificaciones de seguridad y violación de los datos, Privacidad desde el diseño, interés legítimo, limitación del propósito y tratamiento justo.

(1): Véanse las definiciones en la página 58.

Riesgos en caso de incumplimiento

Las personas físicas y jurídicas que no cumplan con la ley y la regulación sobre la protección de datos (por ejemplo, el RGPD) se enfrentan a sanciones y costes, en forma de:

Sanciones penales:

- Encarcelamiento.
- Multa para entidades jurídicas.

Sanciones civiles:

- Daños civiles.

Sanciones administrativas:

- Aviso formal.
- Advertencia.
- Requerimiento.
- Limitación del tratamiento temporal o definitiva.
- Retirada de una certificación o requerimiento de retirar una certificación.
- Suspensión de las transferencias de datos.
- Requerimiento de cesar el tratamiento o retirada de la autorización.
- Publicidad de las sanciones impuestas.
- Sanciones sin aviso formal previo (criterio de urgencia).
- Según la violación, una multa administrativa.

Costes significativos:

- Pérdida de ingresos derivada del daño causado a la reputación.

¿Cuál es la multa administrativa máxima contemplada en el RGPD?

Las multas son discrecionales más que obligatorias. Deben imponerse caso por caso y deben ser "eficaces, proporcionales y disuasorias".

Las multas se basan en los artículos específicos de la Reglamentación que la empresa haya violado.

Los encargados y responsables de los datos se enfrentan a multas administrativas de...

Hasta 10 millones de euros o el 2 % de la facturación mundial anual para las infracciones de:

- Condiciones para el consentimiento de los niños (art. 8);
- Tratamiento que no requiere identificación (art. 11);
- Obligaciones generales de los encargados y responsables. (Arte. 25-39);
  Ausencia de registro de tratamiento de los datos personales, falta de seguridad / no informar sobre violaciones de datos, incumplimiento de las normas sobre subcontratación, falta de protección "desde el diseño" y "por defecto",...
- Certificación (art. 48);
- Organismos de certificación (art.43).

Representa 70 000 000 € para ROQUETTE *

Hasta 20 millones de euros o el 4 % de la facturación mundial anual para infracciones de:

- Principios del tratamiento de datos (art.5 - *lealtad, legalidad, transparencia, finalidad, minimización de datos, datos sensibles*);
- Bases legales para el tratamiento (art.6);
- Condiciones de consentimiento (art. 7);
- Tratamiento de categorías especiales de datos (art. 9);
- Derechos de los titulares de los datos (art. 12-22);
  Violación de las disposiciones sobre los derechos de los individuos
- Transferencias de datos a terceros países (art.44-49).
  Transferencia ilegal de datos personales.

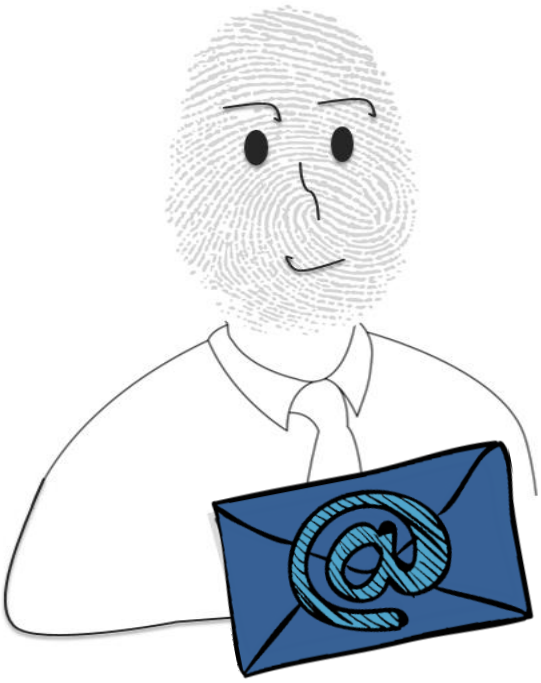
**basado en la facturación de Roquette 2018*

Representa 140 000 000 € para ROQUETTE *

¿Cuáles pueden ser las sanciones penales?

Algunos ejemplos de leyes francesas:

- El acto de recopilar datos personales por medios fraudulentos, injustos o ilegales se castigará con cinco años de prisión y una multa de 300 000 € (Código Penal Art. 226-18).
- Para garantizar un derecho y la protección real del denunciante, la ley anticorrupción (Sapin II) castiga severamente cualquier obstáculo a una alerta. La confidencialidad que rodea la alerta es un elemento esencial de la reglamentación. Por lo tanto, la divulgación de los elementos confidenciales de la alerta (identidad del denunciante, del acusado, información proporcionada en apoyo de la alerta), excepto con respecto a la autoridad judicial, se castiga con dos años de prisión y una multa de 30 000 €.



1 Nuestras normas de RELACIÓN CON LOS TITULARES DE LOS DATOS

Cultura de la privacidad

La **protección de datos** es un conjunto de leyes, reglamentos y buenas prácticas que rigen la recogida y el uso de los datos personales de los individuos.

Por **datos personales** se entenderá toda información relativa a un individuo identificado o identificable.

La **privacidad de los datos** se refiere al tratamiento de los datos personales.

¿A quién afecta?

La privacidad de los datos es relevante para – y la responsabilidad de todas y cada una de las personas de nuestra empresa.

¿Por qué es tan importante?

Los datos sometidos a un mal tratamiento pueden tener graves repercusiones para las empresas, sus empleados y sus clientes.

Las violaciones de la privacidad pueden conducir a sanciones financieras ilimitadas, mala prensa, dañar nuestra reputación, producir la pérdida de confianza de los clientes, pérdidas económicas y, en el caso de los empleados, reclamaciones y tal vez demandas en caso de violaciones de la privacidad de sus propios datos personales y la posibilidad de la aplicación de medidas disciplinarias en otros casos. Todo nuestro interés se centra en tratar los datos de manera apropiada.

Consideramos que:

- Todos los empleados de Roquette tienen que ser conscientes de sus papeles y responsabilidades en lo relativo a la protección de los datos personales. La concienciación aspira a fortalecer la cultura del respeto de la privacidad y la protección de los datos personales dentro de Roquette.

[DDPG001EN – Norma 1]

- Se debe formar a los empleados en la aplicación de la política de protección de los datos personales.

[DDPG001EN – Norma 2]

PIENSE EN LA PRIVACIDAD

¡Es nuestra responsabilidad!

Necesitamos los datos personales de los clientes y empleados para realizar nuestras operaciones con éxito.
Confían en nosotros para que cuidemos esta información esencial.

Todos los empleados tienen la responsabilidad de cumplir las leyes apropiadas sobre Protección de datos.

¡Es nuestra reputación!

La reputación es difícil de ganar y fácil de perder.

Tratar los datos de nuestros clientes y empleados con cuidado y respeto es esencial para proteger nuestra reputación.

TÚ eres nuestra mejor defensa contra el daño a la reputación.

¡Es una cuestión de respeto!

Las elecciones que nuestros clientes y empleados hacen sobre cómo se deben utilizar sus datos personales se deben respetar si queremos conservar la confianza que han depositado en nosotros.

¡Está en nuestras manos!

Todos somos responsables de garantizar que los datos personales de los clientes y empleados se mantengan de forma segura y confidencial.

Se debe tener especial cuidado con toda la información que haya que enviar u obtener fuera de la empresa.

Formamos a nuestros empleados y mejoramos nuestros procesos internos.

- Código de conducta - Privacidad y protección de datos - p. 42 – 43.
- Para los recién llegados: Durante la Incorporación mundial se imparten varias sesiones de información y de e-learning sobre la Protección de datos.
- Para los empleados: Los cursos están cargados en Workday Learning.
- Para los Coordinadores de protección de datos: Se ha compartido documentación en nuestra Comunidad “Red de protección de datos”.
- Para todos: Más información el portal interno > Data Protection.

Tratamiento de los datos personales

El tratamiento de los datos personales significa toda operación o conjunto de operaciones realizadas con datos personales o con conjuntos de datos personales, sea o no a mediante medios automatizados, como la recopilación, el registro, la organización, la estructuración, el almacenamiento, la adaptación o alteración, la recuperación, la consulta, el uso, la publicación mediante transmisión, la divulgación u otra forma de puesta a disposición, la alineación o combinación, la restricción, la supresión o la destrucción.

Un requisito de la Protección de datos (y del RGPD) que tiene que conocer es que se necesita un «fundamento jurídico» para tratar los datos personales.

Según la legislación local, puede haber distintas bases legales.

¿Cuál es mi "fundamento jurídico" para el tratamiento de los datos personales?

Usted tiene que poder responder con claridad a la pregunta:

"¿Cómo ha obtenido mi [información] y por qué se le permite tenerlo?"

Más concretamente, significa que tiene que cumplir al menos una de las seis bases legales para el tratamiento de los datos. En virtud del RGPD, no puede tratar datos a menos que:

1. Consentimiento
2. Contrato
3. Obligación legal
4. Intereses vitales
5. Tarea pública
6. Interés legítimo

Legalidad, equidad y transparencia

Nuestras responsabilidades:

Tenemos que aplicar normas para garantizar el tratamiento legal de los datos personales.

Normas	Referencia Q-Docs	Referencia RGPD
• Actuar con legalidad, equidad y transparencia al recopilar datos	DDPG002EN Norma 1	Art. 5 1. a)
• Demostrar que se respeta el consentimiento de las personas afectadas (cuando sea necesario)	DDPG002EN Norma 2	Art. 7
• Respetar los propósitos determinados durante la recopilación de los datos	DDPG002EN Norma 3	Art. 5 1. b)
• Limitar la información recopilada en papel o en formatos digitales a lo estrictamente necesario	DDPG002EN Norma 4	Art. 5 1. c)
• Limitar la conservación de datos a lo estrictamente necesario	DDPG002EN Norma 5	Art. 5 1. e)
• Tomar medidas para transferir datos personales a terceros países o a organizaciones internacionales	DDPG002EN Norma 6	Art. 44 a 50

Para saber más...

Derechos de los titulares de los datos

Un interesado es un individuo que puede ser identificado, ya sea directa o indirectamente, en concreto haciendo referencia a un identificador como un nombre, un número de identificación, un dato de ubicación, un identificador online, o uno o más factores específicos de la identidad social, cultural, económica, mental, genética, fisiológica o física de dicho individuo.

¿Qué es un "titular de los datos"?

Es el término técnico para el individuo al que hacen referencia los datos personales.

¿Qué es una solicitud de acceso del titular de los datos?

Uno de los principales derechos que las leyes vigentes de Protección de datos proporcionan a los individuos es el derecho a acceder a su información personal.

Una persona puede enviarle una "solicitud de acceso del titular" exigiéndole que le informe sobre la información personal que tiene sobre él/ella y que le proporcione una copia de esa información. En la mayoría de los casos, usted debe responder a una solicitud de acceso del titular válida en los 30 (*) días de calendario posteriores a su recepción.

(*): Este período puede variar según la ley aplicable o la naturaleza de la operación de tratamiento de datos.

¿Cuáles son los demás derechos de los titulares de los datos?

Nuestras responsabilidades:

Tenemos que aplicar normas para garantizar los derechos de los titulares de los datos.

Normas	Referencia Q-Docs	Referencia RGPD
• Asegurarse de que los avisos legales cumplan las obligaciones	DDPG006EN Norma 1	Art. 12
• Permitir que los titulares de los datos ejerzan sus derechos de acceso	DDPG006EN Norma 2	Art. 15
• Permitir que los titulares de los datos ejerzan su derecho a la modificación	DDPG006EN Norma 3	Art. 16
• Permitir que los titulares de los datos ejerzan su derecho a la portabilidad de los datos	DDPG006EN Norma 4	Art. 20
• Permitir que los titulares de los datos ejerzan su derecho a la eliminación ("derecho a ser olvidado/a")	DDPG006EN Norma 5	Art. 17
• Permitir que los titulares de los datos ejerzan su derecho a la limitación del tratamiento	DDPG006EN Norma 6	Art. 18
• Notificar la modificación o la eliminación de los datos personales, o la limitación del tratamiento	DDPG006EN Norma 7	Art. 19
• Controlar la toma de decisiones individual automatizada, incluyendo la determinación de perfiles	DDPG006EN Norma 8	Art. 22

Formamos a nuestros empleados y mejoramos nuestros procesos internos.

Aviso de privacidad

Derecho a ser informado de si se están utilizando los datos personales

Como empleados, debemos informarles, a ustedes y a todos los terceros con los que Roquette tiene una relación, si estamos utilizando sus datos personales.

Deberíamos proporcionar información detallada sobre lo siguiente:

- ¿Por qué Roquette está usando sus datos?
- Qué tipo / tipos de datos utiliza Roquette.
- Cuánto tiempo se conservarán sus datos.
- Sus derechos de información.
- De dónde provienen los datos.
- Información de si Roquette va a transferir sus datos a terceros, incluidos sus nombres y los motivos de la transmisión.
- Información de si va a transferir los datos a otra jurisdicción, incluyendo el país involucrado y qué se hará con los datos.
- Si Roquette está utilizando los datos para la determinación de perfiles (un tipo de tratamiento automatizado donde sus datos personales se utilizan para analizar o predecir cosas como su rendimiento en el trabajo, situación económica, salud).
- Cómo contactar con el Responsable de la protección de datos.
- Si le afecta, su derecho a presentar una queja ante la Autoridad de Supervisión.

Esto se llama **Información sobre la privacidad** o **Aviso de privacidad**.

Deberíamos proporcionarles información sobre la privacidad en el momento en que Roquette recopila sus datos. Si Roquette obtiene sus datos de otra fuente, debe proporcionar información sobre la privacidad. Puede hacerlo en forma de un aviso de privacidad.

Esto se llama **derecho a ser informado**.

Normas	Referencia Q-Docs	Referencia RGPD
• Asegurarse de que los avisos legales cumplan las obligaciones	DDPG006EN Norma 1	Art. 12

Ejemplos:

- Información sobre la privacidad en la página web de Roquette disponible en: https://www.Roquette.com/data-protection.
- Información sobre la privacidad en los procesos de RRHH en Workday@Roquette disponible en ONE: Rincón del Empleado>Workday@Roquette.

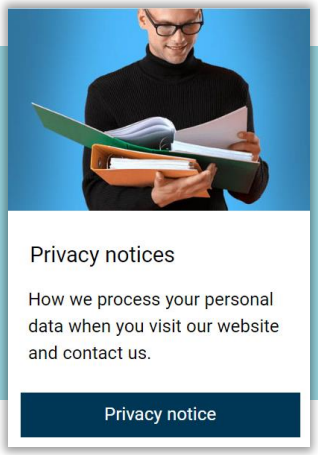
¿Cuándo puede Roquette no informarle de sus actividades?

En general, debemos proporcionarles información sobre la privacidad, pero en algunas circunstancias, no estamos obligados a hacerlo. Estas circunstancias incluyen:

- si ustedes ya disponen de la información sobre la privacidad y nada ha cambiado,
- si es imposible proporcionarles la información sobre la privacidad o si ello requiriese un "esfuerzo desproporcionado", o
- si proporcionarles la información sobre la privacidad imposibilitase el uso de sus datos o fuese perjudicial para las razones de su uso.

Nota: Cuando sean necesarias medidas provisionales para evitar el ocultamiento o la destrucción de pruebas, dicha información podrá emitirse después de la adopción de las medidas provisionales.

Para saber más...



Minimización de los datos

¿Qué es el principio de minimización de los datos?

El Artículo 5(1)(c) del RGPD dice:

> "1. Los datos personales deben ser:
>
> (c) adecuados, pertinentes y limitados a lo estrictamente necesario en relación con los propósitos del tratamiento (minimización de los datos)"

Los formularios en papel o digitales diseñados por las funciones globales para recopilar datos personales deben contener solo los campos de información estrictamente necesarios para el propósito del tratamiento a fin de evitar la recopilación de datos que no están justificados por el tratamiento.

Nuestras responsabilidades:

Debemos asegurarnos de que los datos personales que estamos tratando son:

- adecuados: suficientes para cumplir adecuadamente con su propósito declarado;
- pertinentes: tienen un vínculo racional con ese propósito; y
- limitados a lo necesario: no recopilamos más de lo que necesita para ese propósito.

Normas	Referencia Q-Docs	Referencia RGPD
• Limitar la información recopilada en papel o en formatos digitales a lo estrictamente necesario.	DDPG002EN Norma 4	Art. 5 1. c)

Lista de comprobación:

- ☑ Solo recopilamos datos personales que realmente necesitamos para nuestros fines específicos.
- ☑ Tenemos suficientes datos personales para cumplir adecuadamente esos fines.
- ☑ Revisamos periódicamente los datos que tenemos y eliminamos todos los que no necesitamos.
- ☑ Debemos identificar la cantidad mínima de datos personales que necesitamos para cumplir con nuestro propósito. Deberíamos tener esa cantidad de información, pero no más.

El principio de responsabilidad significa que debemos ser capaces de demostrar que disponemos de los procesos adecuados para asegurarnos de recopilar y conservar los datos personales que necesitamos.

También hay que tener en cuenta que el RGPD dice que las personas tienen derecho a completar cualquier información incompleta que sea inadecuada para su propósito, según el derecho de modificación. También tienen derecho a que eliminemos cualquier información que no sea necesaria para nuestro propósito, según el derecho de eliminación (derecho a ser olvidado).

Formamos a nuestros empleados y mejoramos nuestros procesos internos.

Seguridad de los datos

La **seguridad cibernética** es una actividad transversal cuya aplicación garantiza que los datos se puedan compartir y utilizar con un nivel adecuado y garantizado de protección de la información y los activos relacionados:

- **Confidencialidad**: garantiza que la información se mantenga confidencial y no se divulgue a personas o entidades inapropiadas,
- **Integridad**: protege la exactitud y la integridad de la información y los métodos de tratamiento,
- **Disponibilidad**: garantiza que los usuarios autorizados siempre tengan acceso a la información, las aplicaciones y los servicios, siempre que sea necesario,
- **Trazabilidad**: se refiere a la capacidad de mantener rastros relevantes y, cuando sea necesario, pruebas de lo que se hizo en nuestros sistemas. La trazabilidad también cubre objetivos legales como el no repudio o la rendición de cuentas.

Los activos de información personal incluyen:

- Documentos en papel (textos, mapas, imágenes ...),
- Información digital en entorno de oficina,
- Información digital en entorno móvil,
- Conocimientos y habilidades profesionales (propiedad de individuos o compartidos oralmente),
- Elementos físicos (como muestras, cepas, modelos ...).

[DSUG006EN] Gestión de la Directiva de seguridad cibernética

La **Seudonimización** implica el tratamiento de los datos personales de tal manera que los datos personales ya no puedan atribuirse a un titular específico sin el uso de información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas para garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

La **Anonimización** es el proceso mediante el cual los datos personales se alteran de manera irreversible de tal manera que un titular de los datos ya no pueda ser identificado directa o indirectamente, ya sea por el **encargado** de los datos (1) solo o en colaboración con cualquier otra parte.

El **Cifrado** es el método mediante el cual el texto sin formato o cualquier otro tipo de datos pasa de una forma legible a una versión codificada que solo puede ser decodificada por otra entidad si tiene acceso a una clave de descifrado. El cifrado es uno de los métodos más importantes para proporcionar seguridad de datos, especialmente para la protección de extremo a extremo de los datos transmitidos a través de redes.

(1): Véanse las definiciones en la página 38.

Consideramos que:

Para mantener la seguridad y evitar que el tratamiento infrinja las leyes y reglamentaciones relativas a la protección de datos, Roquette y nuestros subcontratistas debemos evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigar esos riesgos, como el **cifrado** o la **seudonimización**.

Nuestras responsabilidades:

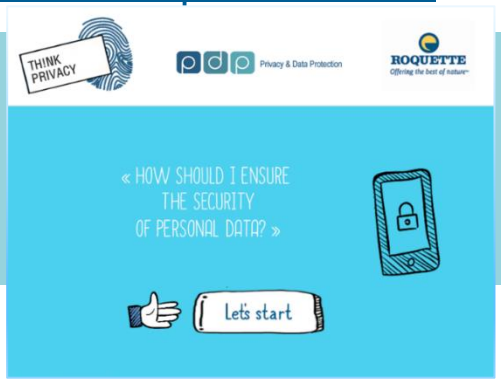
Necesitamos implementar medidas de seguridad cuando manejamos cualquier tipo de datos personales, pero lo que apliquemos dependerá de nuestras circunstancias particulares. Necesitamos garantizar la confidencialidad, la integridad y la disponibilidad de los sistemas y servicios que utilizamos para tratar los datos personales.

Entre otras cosas, esto puede incluir políticas de seguridad de la información, controles de acceso, supervisión de la seguridad y planes de recuperación.

Deben tomarse las medidas de seguridad adecuadas durante todo el ciclo de vida de los datos personales y por parte de todos los interesados.

Normas	Referencia Q-Docs	Referencia RGPD
• Aplicación y revisión de las medidas de seguridad definidas en las políticas y directivas de seguridad	DDPG007EN Norma 1	Art.32
• Integración de la seguridad de la información y la revisión de la protección de datos en los proyectos	DDPG007EN Norma 2	Art.32
• Seguridad, privacidad y protección de datos desde el diseño y por defecto	DDPG007EN Norma 3	Art.25
• Integración de cláusulas de seguridad de la información y de protección de datos con los subcontratistas	DDPG007EN Norma 4	Art.32

Formamos a nuestros empleados y mejoramos nuestros procesos internos.



Información personal Clasificación

Se prohíbe el tratamiento de los datos personales confidenciales y de algunas categorías especiales de datos personales, excepto en casos específicos.

Este tratamiento requiere medidas de protección en términos de:

Marcado, acceso, transmisión, transporte, copia e impresión, almacenamiento y archivado, destrucción.

La **Clasificación** tiene como objetivo identificar los activos de información confidencial, cualquiera sea su naturaleza y su portador, y especificar, si es necesario, medidas de protección para reducir los riesgos después de una publicación no deseada.

El nivel de **Clasificación de la confidencialidad** se relaciona directamente con el impacto evaluado de una divulgación no deseada de la información.

[DSUG001EN] Directiva sobre la Protección de la información

Clasificación de la protección de la información	Tipos de datos personales	Categorías de datos personales
Nivel 1 = RESTRINGIDO ROQUETTE Definición: tipo de información cuya divulgación abierta y amplia no se recomienda	Datos personales comunes	Estado civil, identidad, datos de identificación
		Vida personal (hábitos de vida, estado civil, excluyendo datos sensibles)
		Vida profesional (cv, educación y formación profesional, premios)
		Información económica y financiera (ingresos, situación financiera, situación fiscal)
		Datos de conexión (direcciones IP, registros de eventos)
		Datos de ubicación (viajes, datos GPS, datos GSM)
Nivel 2 = CONFIDENCIAL ROQUETTE Definición: tipo de información cuya divulgación puede dañar significativamente los intereses del grupo	Datos personales percibidos como sensibles	Numero de seguridad social
		Biométricos
		Datos bancarios
Nivel 3 = SECRETO ROQUETTE Definición: tipo de información cuya divulgación puede dañar en gran medida los intereses del grupo	Datos personales sensibles en el sentido de la Ley de Protección de Datos	Opiniones filosóficas, políticas, religiosas y sindicales, vida sexual, datos de salud, origen racial o étnico
		Delitos, condenas, medidas de seguridad.

Nuestras responsabilidades:

Normas	Referencia Q-Docs	Referencia RGPD
• Respetar el marco legal para el tratamiento de los datos confidenciales	DDPG004EN Norma 1	Art.9
• Prohibir el tratamiento de los datos sobre condenas penales y delitos	DDPG004EN Norma 2	Art.10
• Limitar el acceso a los datos de salud solo a los profesionales autorizados	DDPG004EN Norma 3	Art.9
• Prohibir el uso del número de identificación nacional como identificador único	DDPG004EN Norma 4	Art.87
• Restringir el acceso y el uso de los datos bancarios	DDPG004EN Norma 5	Art.9
• Restringir el acceso a los datos confidenciales solo a las personas autorizadas	DDPG004EN Norma 6	Art.9
• Realizar evaluaciones del impacto en la privacidad de los titulares de los datos involucrados en el tratamiento de los datos confidenciales	DDPG004EN Norma 7	Art.35
• Limitar el uso del campo de comentarios a la información general	DDPG004EN Norma 8	Buena práctica

Algunos consejos prácticos...

Ejemplos de medidas de protección que deben tomarse para cada categoría de activos de información clasificada (papel, digital, saber hacer, física).

Conservación de datos

La creciente necesidad de desmaterializar las operaciones y el intercambio de información entre el Grupo, nuestros clientes y nuestros socios comerciales, así como los requisitos legales y reglamentarios, han sometido a Roquette a una serie de obligaciones en términos de la duración del período de conservación de los datos y de las políticas de gestión de los registros.

Según nuestras actividades, Roquette adquiere y trata una gran cantidad de datos confidenciales relacionados con nuestra estrategia, nuestros resultados financieros, nuestro desarrollo comercial o nuestros compromisos, así como de **datos personales relacionados con nuestros clientes, socios comerciales y miembros del personal**.

La información enviada o recibida por Roquette en relación con nuestras actividades debe conservarse durante un plazo mínimo de retención, a pesar de que nada impide que la empresa los conserve en los archivos durante plazos más largos, **excepto en caso de que contengan información personal**.

Este límite de tiempo, durante el cual las autoridades administrativas y competentes pueden realizar inspecciones posteriores, varía según la naturaleza de la información conservada y los requisitos legales correspondientes.

Se prohíben los plazos de almacenamiento infinitos o indeterminados.

RGPD Art. 5 1. E)

"limitación del almacenamiento"

Los datos personales se conservarán de forma que permita la identificación de los interesados por un tiempo no superior al que sea necesario para los propósitos para los que se tratan los datos personales.

Los datos personales pueden almacenarse durante períodos más largos en la medida en que los datos personales se traten solamente con fines de archivado en interés público, propósitos de investigación científica o histórica o fines estadísticos sujetos a la aplicación de las medidas técnicas y organizativas apropiadas necesarias para salvaguardar los derechos y libertades del titular de los datos.

Nuestras responsabilidades:

- Como encargado de los datos, Roquette debe definir plazos de almacenamiento específicos y adecuados para cada categoría de datos personales recopilados y tratados.
- Antes de llevar a cabo el tratamiento de los datos personales, el propietario del proyecto con la asistencia de un coordinador de Protección de Datos debe especificar en nuestro registro, la duración de la retención de datos.
- Debemos conservar los datos personales solo durante el tiempo necesario para su tratamiento y cumplir las leyes aplicables.

Normas	Referencia Q-Docs	Referencia RGPD
• Limitar la conservación de datos a lo estrictamente necesario	DDPG002EN Norma 5	Art. 5 1. E)

A este respecto, las funciones globales, las GBU y las áreas se comprometen a cumplir con las reglas de retención de información de la compañía y a mantener los procedimientos asociados en condiciones operativas.

Ejemplo:

Al final del proceso de selección de personal, debemos eliminar la información sobre los candidatos no seleccionados, a menos que acepten permanecer en nuestro "polo" durante un período limitado (2 años).

Formamos a nuestros empleados y mejoramos nuestros procesos internos.

2 Nuestras normas de RELACIÓN CON LOS AFILIADOS Y SUBCONTRATISTAS

Cualificación de responsable y encargado

El **Encargado** es la persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o junto con otros, determina los propósitos y medios del tratamiento de los datos personales.

El **Encargado conjunto** son dos o más encargados que determinan conjuntamente los propósitos y los medios de tratamiento. Sin embargo, independientemente de esos acuerdos, cada encargado sigue siendo responsable de cumplir con todas las obligaciones de los encargados plasmadas en el RGPD.

El **Responsable** es una persona física o jurídica, autoridad pública, agencia u otro organismo que procesa datos personales en nombre del encargado.

¿Quién es el Responsable en el sentido del Reglamento general de protección de datos?

(Artículo 4 del RGPD – Definiciones).

Una gran variedad de proveedores de servicios tiene la capacidad de ser responsable en el sentido legal del término. Las actividades de los responsables pueden referirse a una tarea muy específica (subcontratación de la entrega de correo) o ser más generales y de mayor alcance (gestión de todo el servicio en nombre de otra organización, como la gestión de la remuneración de los empleados, por ejemplo).

Los siguientes se ven particularmente afectados por el RGPD:

- Proveedores de servicios de TI (alojamiento, mantenimiento, etc.), integradores de software, compañías de seguridad cibernética o empresas de consultoría de TI (anteriormente conocidas como empresas de servicios de ingeniería de TI) que tienen acceso a los datos,
- agencias de marketing o de comunicación que tratan datos personales en nombre de los clientes, y
- de manera más general, cualquier organización que preste un servicio que implique el tratamiento de datos personales en nombre de otra organización,
- una autoridad pública o asociación también puede considerarse como tal.

En la medida en que no tengan acceso o traten datos personales, los editores de software y los fabricantes de equipos (como terminales de marcado, equipos biométricos o equipos médicos) no se ven afectados.

Ejemplo de calificación de responsable y encargado:

La empresa A presta un servicio de entrega de cartas de marketing utilizando los archivos de datos de clientes de las empresas B y C.

La empresa A es responsable para las empresas B y C en la medida en que trata los datos de clientes necesarios para enviar las cartas en nombre de las empresas B y C.

Las empresas B y C son los encargados de gestión de sus clientes, incluso en lo que respecta a la entrega de las cartas de marketing.

La empresa A también es la encargada de la gestión del personal que emplea y de la gestión de sus clientes, que incluye las empresas B y C.

Texto oficial

- Artículo 4 del RGPD para las definiciones de responsable y encargado
- Artículo 28.10 del RGPD sobre la noción de encargado

Formamos a nuestros empleados y mejoramos nuestros procesos internos

Cláusulas de protección de datos

¿Cuándo se necesita un contrato y por qué es importante?

Siempre que, como encargados, usemos a un responsable para tratar los datos personales en nuestro nombre, debe existir un contrato escrito entre las partes. El contrato es importante para que ambas partes entiendan sus responsabilidades y obligaciones.

Los contratos con cláusulas específicas de protección de datos y / o acuerdos de protección de datos entre Roquette, como encargado, y sus responsables aseguran que ambos comprendamos nuestras obligaciones, responsabilidades y compromisos. Los contratos también nos ayudan a cumplir el RGPD, y nos ayudan a demostrar a los individuos y a los reguladores nuestro cumplimiento según exige el principio de responsabilidad.

¿Qué responsabilidades y compromisos tenemos como encargados cuando usamos un responsable?

Solo debemos usar responsables que puedan brindar garantías suficientes de que aplicarán las medidas técnicas y organizativas apropiadas para garantizar que su tratamiento cumpla con los requisitos de RGPD y proteja los derechos de los titulares de los titulares de los datos.

Como encargados, somos los principales responsables del cumplimiento general del RGPD y de otras leyes vigentes relativas a la privacidad, y de demostrar ese cumplimiento. Si esto no se logra, podemos vernos obligados a pagar daños y perjuicios en procedimientos legales o estar sujetos a multas u otras sanciones o medidas correctivas.

¿Qué novedades presenta el RGPD?

El RGPD establece que los contratos escritos entre encargados y responsables son una exigencia, en lugar de una simple forma de demostrar el cumplimiento del principio de protección de datos (medidas de seguridad apropiadas) según las leyes de protección de datos vigentes.

En la actualidad, estos contratos deben incluir unos términos mínimos específicos. Estos términos están destinados a garantizar que el tratamiento realizado por un responsable cumpla con todos los requisitos del RGPD, no solo los relacionados con la seguridad de los datos personales.

Norma	Referencia Q-Docs	Referencia RGPD
• Integración de cláusulas de seguridad de la información y de protección de datos con los subcontratistas	DDPG007EN Norma 4	Art. 32
• Seguridad de los contratistas	DSUG016EN	

¿Qué debe incluirse en el contrato?

Los contratos deben establecer:

- ☑ el tema y la duración del tratamiento;
- ☑ la naturaleza y el propósito del tratamiento;
- ☑ el tipo de datos personales y las categorías de titulares de los datos; y
- ☑ las obligaciones y derechos del encargado.

Los contratos también deben incluir términos o cláusulas específicas con respecto a:

- ☑ el tratamiento solo según las instrucciones documentadas del encargado;
- ☑ el deber de confianza;
- ☑ las medidas de seguridad apropiadas;
- ☑ el uso de subresponsables;
- ☑ los derechos de los titulares de los datos;
- ☑ la asistencia al encargado;
- ☑ las disposiciones de finalización del contrato; y
- ☑ las auditorías e inspecciones.

Formamos a nuestros empleados y mejoramos nuestros procesos internos.

- Guía sobre la protección de datos para subcontratantes en conformidad con el RGPD.
- Modelo se cláusulas contractuales de la subcontratación en nuestro Privacy Management System: OneTrust@Roquette > Vendor Risk Management módulo.

Acuerdo de transferencia de datos

Una **Transferencia de datos** es cualquier comunicación, copia o tránsito de datos personales (como servidores de alojamiento, envío de archivos adjuntos por correo electrónico, herramientas de acceso remoto, uso compartido de pantalla, etc.) destinados al tratamiento en otros países que no tienen las mismas leyes de protección de datos personales aplicables.

Estamos más conectados que nunca. Para Roquette, que opera a escala mundial, la transferencia internacional de datos es un elemento esencial de las operaciones comerciales diarias. Roquette, por ejemplo, almacena datos personales de empleados en un servicio en la nube alojado en el extranjero y comparte datos personales de empleados y clientes entre sus filiales situadas en todo el mundo.

¿Cómo afectarán el RGPD y las demás leyes de protección de datos vigentes a tales transferencias internacionales de datos?

Nuestras responsabilidades:

Cualquier transferencia de datos personales que estén siendo tratados o que vayan a serlo después de la transferencia a un tercer país o a una organización internacional solo tendrá lugar si:

- La ley local lo permite y / o la autoridad de supervisión ha decidido que el tercer país, un territorio o uno o más sectores específicos dentro de ese tercer país, o la organización internacional en cuestión garantiza un nivel adecuado de protección o ha otorgado su autorización, y /o

- Se toma una medida legal (por ejemplo: Normas corporativas vigentes o cláusulas contractuales estándar para la transferencia de datos personales a responsables situados en terceros países en virtud de la Directiva 95/46 / CE del Parlamento Europeo y del Consejo, etc.).

Norma	Referencia Q-Docs	Referencia RGPD
• Tomar medidas para transferir datos personales a terceros países o a organizaciones internacionales	DDPG002EN Norma 6	Art. 44 a 50

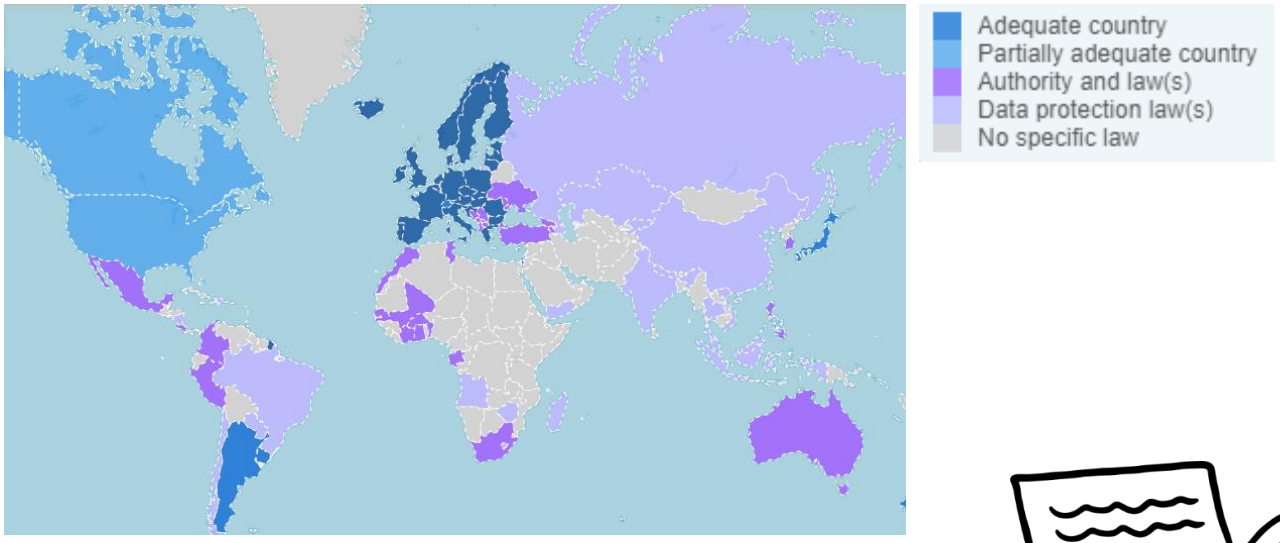
En todos los casos, póngase en contacto primero con el Responsable de la protección de datos.

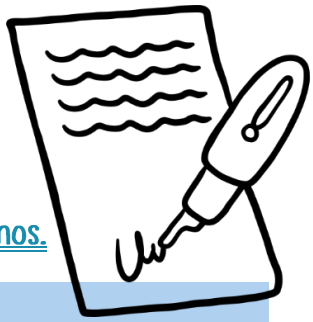
¿A qué países podemos transferir los datos personales y en qué condiciones?

Para obtener una descripción general, consulte este mapa:

https://www.cnil.fr/en/data-protection-around-the-world.

Este mapa le permite ver el nivel de protección de datos de cada país.





Formamos a nuestros empleados y mejoramos nuestros procesos internos.

- Data Transfer Agreement incluida en nuestra plantilla “Data Processing Agreement”.
- Preguntas frecuentes para abordar algunas cuestiones planteadas por la entrada en vigor de la Decisión de la Comisión de la UE sobre cláusulas contractuales estándar para la transferencia de datos personales a responsables situados en terceros países.

3 Nuestras normas de RELACIÓN CON nuestra RED y las AUTORIDADES DE SUPERVISIÓN

Responsable de protección de datos

El Grupo ha nombrado a un Responsable de protección de datos.

El Responsable de protección de datos o DPO nos ayuda a supervisar la conformidad interna, nos informa y nos asesora en lo relativo a nuestras obligaciones de protección de datos, ofrece consejos sobre las Evaluaciones del impacto en la protección de datos (EIPD) y actúa como punto de contacto para los titulares de los datos y la autoridad de supervisión.

El DPO debe ser independiente, experto en protección de datos, disponer de las fuentes suficientes e informar al nivel jerárquico más alto.

El DPO nos puede ayudar a demostrar el cumplimiento, y forma parte del enfoque reforzado basado en la responsabilidad.

Tareas del DPO	Referencia Q-Docs	Referencia RGPD
• Nuestro DPO tiene la tarea de supervisar el cumplimiento del RGPD y otras leyes de protección de datos, nuestras políticas de protección de datos, de concienciación, de formación y las auditorías.	MDPG001EN Manual de protección de datos personales	RGPD Artículo 39 Tareas del responsable de protección de datos
• Tendremos en cuenta los consejos de nuestro DPO y la información que proporciona sobre nuestras obligaciones de protección de datos.		
• Cuando llevamos a cabo una EIPD, buscamos el asesoramiento de nuestro DPO, que también supervisa el proceso.		
• Nuestro DPO actúa como punto de contacto para las autoridades de supervisión.		
• Al realizar sus tareas, nuestro DPO tiene debidamente en cuenta el riesgo asociado a las operaciones de tratamiento y tiene en cuenta la naturaleza, el alcance, el contexto y los propósitos de dicho tratamiento.		

El CEO del Grupo designó ante la CNIL al DPO, quien tomó posesión de su cargo el 25 de mayo de 2018, fecha de aplicación del RGPD.

Accesibilidad del DPO:

- Nuestra Responsable de protección de datos, Jennifer Godin, es fácilmente accesible como punto de contacto para nuestros empleados, los individuos y la Autoridad de supervisión.

- Hemos publicado los datos de contacto del DPO y se los hemos comunicado a las Autoridades de supervisión.

  ☑ https://www.roquette.com/data-protection
  ☑ ONE > Funciones globales > Protección de datos
  ☑ ONE > Nuestra comunidad > Red de protección de datos

Póngase en contacto con el DPO en caso de:

☑ Tratamiento de datos personales

☑ Solicitudes de los titulares de los datos

☑ Violación de los datos personales

☑ Necesidad de asesoramiento o asistencia

Un punto de contacto único: dpo@Roquette.com o jennifer.godin@Roquette.com

Formamos a nuestros empleados y mejoramos nuestros procesos internos.

Red de protección de datos

Los enlaces de los departamentos y los DPO o coordinadores locales son una red que permite al Responsable de protección de datos del Grupo, respectivamente, aplicar las normas de Protección de datos personales en cada unidad de negocio y departamento de soporte, y cumplir con los requisitos de las leyes y regulaciones relevantes de protección de datos en los países donde opera el Grupo.

Los DPO / coordinadores locales tendrán al menos las siguientes tareas:

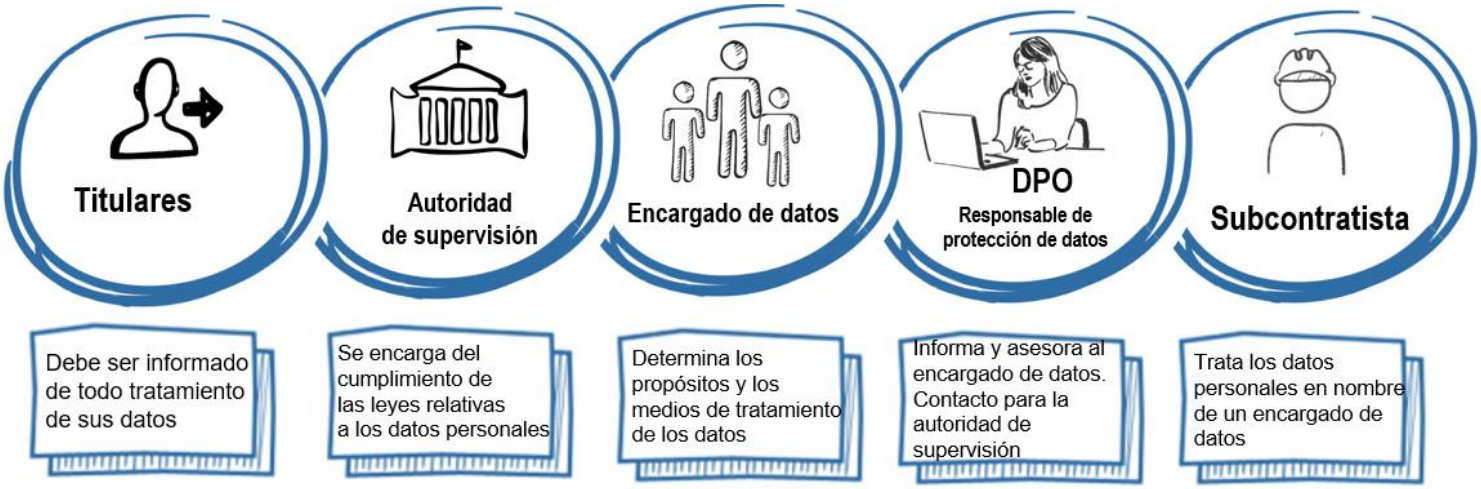
- Informar y asesorar localmente sobre las obligaciones de cumplimiento de la Política de protección de datos personales de Roquette definida por el DPO del Grupo Roquette y los requisitos de sus leyes locales aplicables en materia de protección de datos;
- Para supervisar el cumplimiento de la legislación local, así como de otras legislaciones y regulaciones aplicables con respecto a la protección de datos, cuando sea necesario, con la asistencia del DPO del Grupo Roquette y con las políticas relacionadas con la protección de datos personales;
- Ofrecer asesoramiento local, cuando se solicite, con respecto a la evaluación del impacto en la protección de datos y supervisar su desempeño de cumplimiento;
- Cooperar con la autoridad de supervisión local;
- Actuar como punto de contacto para el DPO del Grupo Roquette en asuntos relacionados con el tratamiento y consultar al DPO del Grupo Roquette, cuando corresponda, con respecto a cualquier otro asunto;
- Informar sus actividades al DPO del Grupo Roquette para contribuir al Sistema de gestión de la protección de datos del Grupo.

Formamos a nuestros empleados y mejoramos nuestros procesos internos.

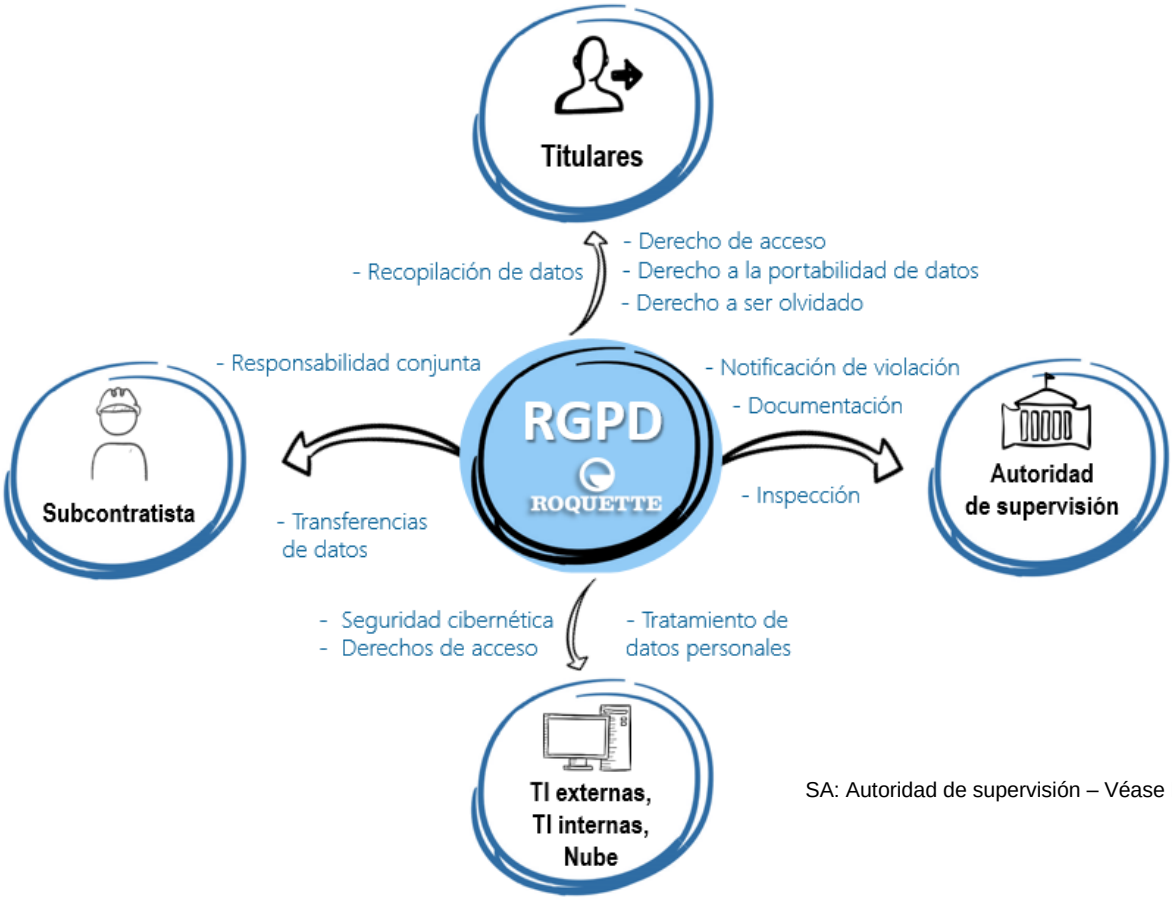
- Nuestro seminario anual PDP es el punto de encuentro de nuestra red de colaboradores en materia de protección de datos y privacidad.

y Partes interesadas

¿Quiénes son los nuevos actores?



¿Cuáles son las relaciones entre las partes interesadas?



SA: Autoridad de supervisión – Véase la página 50

Autoridades de supervisión

En todo el mundo, muchos países disponen de una ley de protección de datos y de una **Autoridad de protección de datos (DPA)** independiente.

Estas autoridades son el regulador nacional independiente de la privacidad y la libertad de información. Promueven y defienden los derechos de los interesados a acceder a la información de las organizaciones y a la protección de su información personal.

¿Cuál es el papel de una autoridad de supervisión en el contexto del RGPD?

Cada Estado miembro dispondrá que una o más autoridades públicas independientes sean responsables de controlar la aplicación de las leyes de datos personales y privacidad, a fin de proteger los derechos y libertades fundamentales de los titulares de los datos en el ámbito del tratamiento de datos personales y facilitar la libre circulación de dichos datos personales dentro de la UE.

En el contexto del RGPD, todos los Estados miembros de la UE tienen una autoridad de protección de datos, que en general sirve como el principal punto de contacto de las partes interesadas dentro de ese Estado miembro.

Para asegurarse de que el RGPD se aplique de manera coherente en toda la UE, cada autoridad de supervisión debe trabajar junto con las demás y con la Comisión Europea.

Cada autoridad de supervisión debe promover en su territorio la concienciación pública y la comprensión de los riesgos, normas, salvaguardas y derechos en relación con el tratamiento de los datos personales.

También son el lugar al que acudir en caso de violación de la legislación de protección de datos y para obtener asesoramiento y respuestas a preguntas específicas y / o asistencia desde la perspectiva de las organizaciones.

En resumen, las responsabilidades de las Autoridades de supervisión (SA) son:

- Garantizar la aplicación de las normas, incluso mediante multas,
- Aclarar la aplicación de las normas si es necesario, p. ej. través de directrices,
- Promover una cultura de diálogo con todas las partes interesadas, incluidas las empresas,
- Cooperar juntas.

CNIL : Commission Nationale de l'Informatique et des Libertés - DPA francesa.

Autoridad principal

- La autoridad de supervisión para el establecimiento principal del encargado o responsable debe actuar como autoridad principal. Debe cooperar con las demás autoridades implicadas.
- La identificación de una autoridad de supervisión principal solo es relevante cuando un encargado o responsable está llevando a cabo un tratamiento transfronterizo de datos personales.

¿Cómo identificar la "autoridad de supervisión principal"?

Identificar el lugar de administración central del encargado principal en la UE.
La autoridad de supervisión del país donde se encuentra el lugar de la administración central es la autoridad principal del encargado.

La **CNIL** *es la autoridad de supervisión principal de Roquette*

¿Cómo funciona el mecanismo de sanción del RGPD en la práctica?

Gobernanza

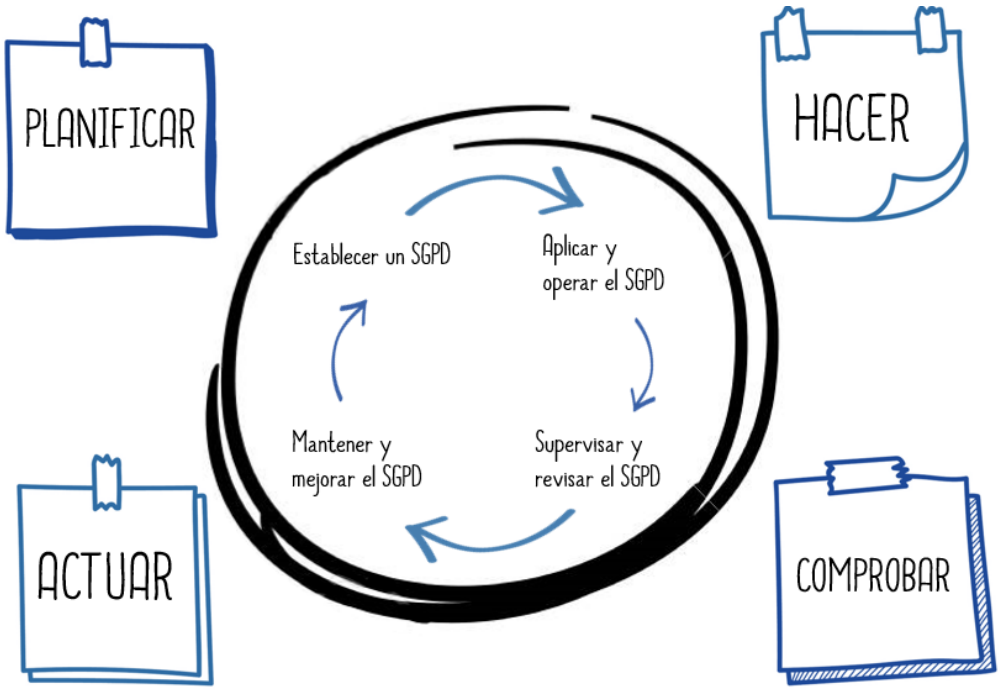
"La **organización de la protección de datos** se estructura principalmente en torno al Responsable de protección de datos, sus coordinadores por centro y por función, el Director Ejecutivo como Encargado de los datos, los Head of Global Functions como responsables de la aplicación del tratamiento de los datos personales y los subcontratistas como Responsable". [MDPG001EN]

Adoptamos un enfoque de proceso para establecer, aplicar, operar, supervisar, revisar, mantener y mejorar el Sistema de gestión de la protección de los datos personales (SGPD) de Roquette.

El proceso y el enfoque para la gestión de la protección de los datos personales definidos en esta gobernanza incita a sus usuarios a acentuar la importancia de:

1) comprender los requisitos de la protección de datos de Roquette y la necesidad de establecer directivas y procedimientos para la protección de datos;
2) aplicar y operar controles para administrar los riesgos de la protección de datos de Roquette en el contexto de los riesgos comerciales generales de Roquette;
3) supervisar y revisar el desempeño y la eficacia del SGDP; y
4) mejora continua basada en la medición objetiva.

Adoptamos el modelo del "Ciclo de Deming" (PDCA), que se aplica para estructurar todos los procesos del Sistema de gestión de la protección de datos (SGPD).



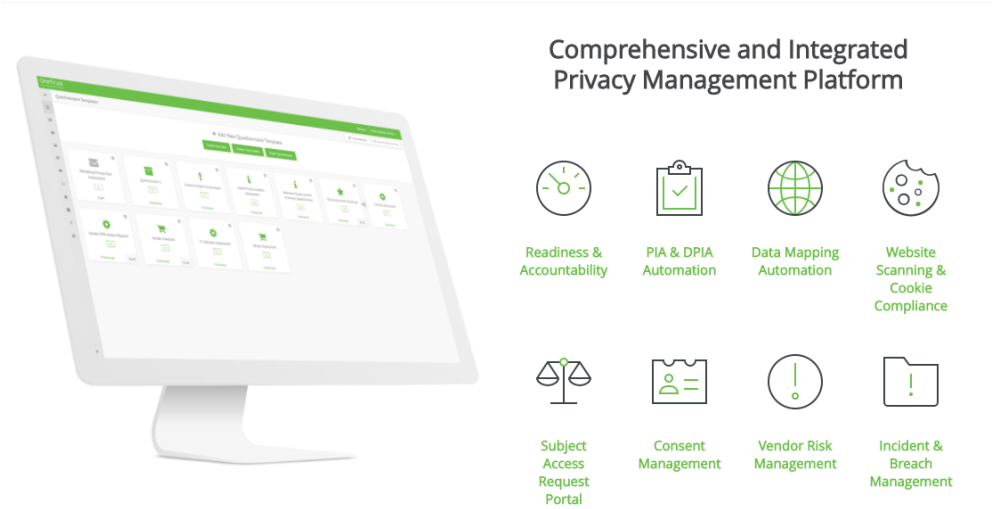
Nuestro enfoque:

Nuestro Programa de cumplimiento del RGPD se centra en:

- Entender cómo nuestra organización recaba, almacena, usa y transfiere los datos para cumplir con el reglamento,
- Generar una cultura de cumplimiento normativo en nuestra organización,
- Llevar a cabo evaluaciones del impacto en la privacidad,
- Prepararse ante violaciones de datos,
- Asignar recursos al Programa de privacidad,
- Implementar un Sistema de gestión de protección de datos (Ciclo de Deming - PDCA).

Para lograr estos objetivos, y como parte de nuestro Programa, hemos:

- definido una política de protección de datos y sus correspondientes gobernanza y documentación,
- gestionado un proyecto de cumplimiento del RGPD para la revisión del tratamiento, la gestión de las violaciones de datos, la revisión de los contratos, cláusulas sobre protección de datos, acuerdo de transferencia de datos, etc.
- implantado un software de administración de la privacidad que cumple con el RGPD.



Las características principales de esta plataforma de gestión son:

- Mantenimiento del registro de tratamiento de datos (mapeo de datos),
- Gestión de los riesgos asociados al tratamiento (de la evaluación del impacto en la privacidad, etc.),
- Gestión de solicitudes y derechos (acceso, modificación, oposición, etc.),
- Gestión de los incidentes y las violaciones de datos,
- Gestión de la documentación de cumplimiento.

Responsabilidad

La **Responsabilidad** es uno de los principios de la protección de datos. Nos hace responsables de cumplir con el RGPD y dice que debemos poder demostrar nuestro cumplimiento.

¿Por qué es importante la responsabilidad?

Asumir la responsabilidad de lo que hacemos con los datos personales y demostrar las medidas que hemos tomado para proteger los derechos de las personas no solo da lugar a un mejor cumplimiento de la ley, sino que también nos ofrece una ventaja competitiva. La responsabilidad es una oportunidad real para mostrar y demostrar cómo respetamos la privacidad de las personas. Esto puede ayudarnos a desarrollar y a conservar la confianza de las personas.

Además, si algo sale mal, ser capaces de demostrar que consideramos activamente los riesgos y establecimos medidas y salvaguardas puede ayudarnos a mitigar cualquier posible acción judicial. Por otro lado, si no podemos mostrar buenas prácticas de protección de datos, podemos quedar expuestos a multas y dañar nuestra reputación.

¿Qué significa concretamente adherirse al principio de responsabilidad?

El tratamiento de datos personales implica un deber de cuidado y la adopción de medidas concretas y prácticas para su protección. Adherirse al principio de responsabilidad significa:

- documentar y comunicar, según corresponda, todas las directivas, procedimientos y prácticas relacionadas con la privacidad (nuestra "Política");
- asignar a un individuo específico dentro de la organización (que a su vez podría delegar a otros en la organización según corresponda) la tarea de aplicar la Política;
- al transferir datos personales a terceros, asegurarnos que el tercero destinatario estará obligado a proporcionar un nivel equivalente de privacidad y de protección de datos mediante medios contractuales u otros, como políticas internas obligatorias (la ley aplicable puede contener requisitos adicionales con respecto a las transferencias internacionales de datos);
- proporcionar la formación adecuada al personal del encargado de datos que tendrá acceso a los datos personales;

- establecer procedimientos eficientes de gestión de las reclamaciones internas y los procedimientos de reparación para el uso del titular de los datos;
- informar a los titulares de los datos sobre las violaciones de la privacidad que pueden ocasionarles daños sustanciales (a menos que esté prohibido, por ejemplo, si se trabaja con la policía), así como las medidas adoptadas para su resolución;
- notificar a todas las partes interesadas relevantes relacionadas con la privacidad las violaciones de la privacidad según lo requerido en algunas jurisdicciones (por ejemplo, las autoridades de protección de datos) y según el nivel de riesgo;
- permitir a un titular de los datos perjudicado el acceso a sanciones y / o remedios apropiados y eficaces, como la modificación, la cancelación o la restitución si se ha producido una violación de la privacidad; y
- considerar los procedimientos de compensación por situaciones en las que será difícil o imposible restablecer el estado de privacidad de la persona física como si no hubiera ocurrido nada.

Lista de comprobación:

- ☑ Asumimos la responsabilidad de cumplir con el RGPD, al más alto nivel de gestión y en toda nuestra organización.
- ☑ Conservamos pruebas las medidas que adoptamos para cumplir el RGPD.

Aplicamos las medidas técnicas y organizativas apropiadas, tales como:

- ☑ adoptar y aplicar las normas de protección de datos;
- ☑ adoptar un enfoque de "protección de datos desde el diseño y por defecto", aplicando las medidas de protección de datos adecuadas durante todo el ciclo de vida de nuestras operaciones de tratamiento;
- ☑ establecer contratos escritos con organizaciones que tratan los datos personales en nuestro nombre;
- ☑ conservar documentación de nuestras actividades de tratamiento;
- ☑ aplicar las medidas de seguridad apropiadas;
- ☑ registrar y, cuando sea necesario, informar de las violaciones de los datos personales;
- ☑ llevar a cabo evaluaciones de impacto en la protección de datos para los usos de datos personales que puedan dar lugar a un alto riesgo para los intereses de las personas;
- ☑ nombrar a un responsable de protección de datos; y
- ☑ adherirse a los códigos de conducta relevantes y suscribirse a mecanismos de certificación (cuando sea posible).

- ☑ Revisamos y actualizamos nuestras medidas de responsabilidad con una frecuencia apropiada.

Documentación

¿Cuál es la documentación?

Estamos obligados a conservar un registro de nuestras actividades de tratamiento que abarquen áreas como los propósitos del tratamiento, el intercambio de datos y la retención; todo esto recibe el nombre de **documentación**.

Es importante documentar nuestras actividades de tratamiento, no solo porque es un requisito legal en sí, sino también porque puede respaldar la buena gobernanza de los datos y ayudarnos a demostrar nuestro cumplimiento de otros aspectos del RGPD y de las leyes de protección de datos vigentes.

Lista de comprobación:

Documentación de las actividades de tratamiento: requisitos

- ☑ Como encargado de los datos personales que tratamos, documentamos toda la información aplicable de conformidad con el Artículo 30 (1) del RGPD.
- ☑ Documentamos nuestras actividades de tratamiento por escrito.
- ☑ Documentamos nuestras actividades de tratamiento de forma granular con enlaces significativos entre los diferentes documentos de información.
- ☑ Realizamos revisiones periódicas de los datos personales que tratamos y actualizamos nuestra documentación en consecuencia.

Documentación de las actividades de tratamiento: buena práctica

- ☑ Documentamos nuestras actividades de tratamiento en formato electrónico para poder añadir, eliminar y modificar la información fácilmente.

Cuando nos preparamos para documentar nuestras actividades de tratamiento, nosotros:

- ☑ realizamos auditorías de información para averiguar qué datos personales posee nuestra organización;
- ☑ utilizamos cuestionarios a través de nuestras herramientas digitales, de seguridad y privacidad y hablamos con el personal de toda la organización para obtener una imagen más completa de nuestras actividades de tratamiento; y
- ☑ revisamos nuestras políticas, directivas, procedimientos, contratos y acuerdos para abordar áreas como la retención, la seguridad y el intercambio de datos.

En el marco de nuestro registro de actividades de tratamiento, documentamos o vinculamos con la documentación:

- ☑ la información requerida para los avisos de privacidad;
- ☑ los registros de consentimiento cuando sea necesario;
- ☑ los contratos encargado-responsable;
- ☑ la ubicación de los datos personales;
- ☑ los informes de Evaluación del impacto en la protección de datos; y también
- ☑ los registros de violaciones de los datos personales;
- ☑ los registros de solicitudes de los titulares de los datos.

¿Dónde está nuestra documentación sobre la Protección de datos?

ONE
Funciones globales
Protección de datos

Privacy & Data Protection

"La protección de los datos es relevante y es la responsabilidad de todas y cada una de las personas de nuestra empresa"

Contenido

- Leyes y reglamentaciones
- Información y concienciación
- Buenas prácticas y políticas

ONE
Comunidad
Red de protección de datos

Data Protection Network

"Todos participamos en la protección de los datos personales"

Contenido

- Política de protección de datos personales
- Sistema de gestión de la protección de datos
- Legislación local
- Recursos humanos
- Digital Global
- Departamento jurídico y de conformidad
- Auditoría y Control Interno
- GBU y Comercial
- Innovación, I+D
- Seguridad mundial
- Seguros y Gestión de riesgo

OneTrust
Software de gestión de la privacidad

OneTrust
Privacy Management Software
@ ROQUETTE

"Nuestra herramienta de gestión de la privacidad dedicada a la seguridad de la privacidad y al riesgo procedente de terceros"

Módulos

Data Mapping Automation
PIA & DPIA Automation
Subject Access Request Portal
Incident & Breach Management

CULTURA

CUMPLIMIENTO

RESPONSABILIDAD

Evaluación de impacto en la privacidad

La **Evaluación del impacto en la privacidad** o **PIA** es un proceso destinado a describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas que resultan del tratamiento de los datos personales evaluándolos y determinando las medidas para hacerles frente.

El acrónimo "**PIA**" se usa indistintamente para referirse a la **Evaluación del impacto en la privacidad** y la **Evaluación del impacto en la protección de datos (DPIA)**.

¿Cómo se realiza una Evaluación del impacto en la privacidad (PIA)?

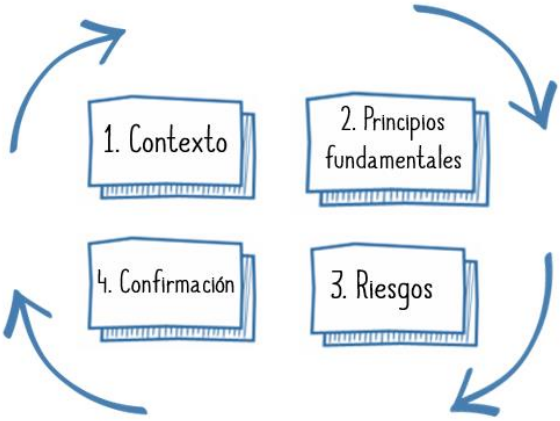
El enfoque de cumplimiento aplicado mediante la realización de una PIA se basa en dos pilares:

1) **derechos y principios fundamentales**, que son "no negociables", establecidos por ley y que deben respetarse, independientemente de la naturaleza, la gravedad y la probabilidad de los riesgos;
2) **gestión de los riesgos de privacidad de los titulares de los datos**, que determina los controles técnicos y organizativos adecuados para proteger los datos personales.

Enfoque de cumplimiento utilizando una PIA

En resumen, para llevar a cabo una PIA es necesario:

1) definir y describir el contexto del tratamiento de los datos personales que se está considerando;
2) analizar los controles que garantizan el cumplimiento de los principios fundamentales: la proporcionalidad y la necesidad de tratamiento, y la protección de los derechos de los titulares de los datos;
3) evaluar los riesgos de privacidad asociados con la seguridad de los datos y garantizar que se traten adecuadamente;
4) documentar formalmente la validación de la PIA en vista de los hechos anteriores o decidir la revisión de los pasos anteriores.



Enfoque general para llevar a cabo una PIA

Se trata de un proceso de mejora continua. Por lo tanto, a veces se requieren varias iteraciones para lograr un sistema de protección de privacidad aceptable. También requiere una supervisión de los cambios a lo largo del tiempo (en contexto, controles, riesgos, etc.), por ejemplo, cada año, y actualizaciones cada vez que se produzca un cambio significativo.

El enfoque debe implementarse tan pronto como se diseñe un nuevo tratamiento de datos personales. Aplicar este enfoque desde el principio permite determinar los controles necesarios y suficientes y optimizar así los costes. Por el contrario, aplicarlo después de la creación del sistema y la ejecución de los controles puede cuestionar las elecciones realizadas.

Nuestras responsabilidades:

- Cuando un tipo de tratamiento, en particular mediante el uso de nuevas tecnologías, y teniendo en cuenta la naturaleza, el alcance, el contexto y los propósitos del tratamiento, pueda dar lugar a un alto riesgo para los derechos y libertades de las personas físicas, Roquette como encargado, debe, previamente al tratamiento, realizar una evaluación del impacto de las operaciones de tratamiento previstas en la protección de los datos personales.
- El propietario del proyecto deberá buscar el asesoramiento del Responsable de protección de datos designado al realizar una evaluación de impacto de protección de datos.

Normas	Referencia Q-Docs	Referencia RGPD
• Llevar a cabo una PIA en caso de alto riesgo	DDPG003EN Norma 1	Art. 35
• Contenido de la PIA	DDPG003EN Norma 2	
• Tareas del DPO relativas a la PIA	DDPG003EN Norma 3	
• Revisión de la PIA	DDPG003EN Norma 4	

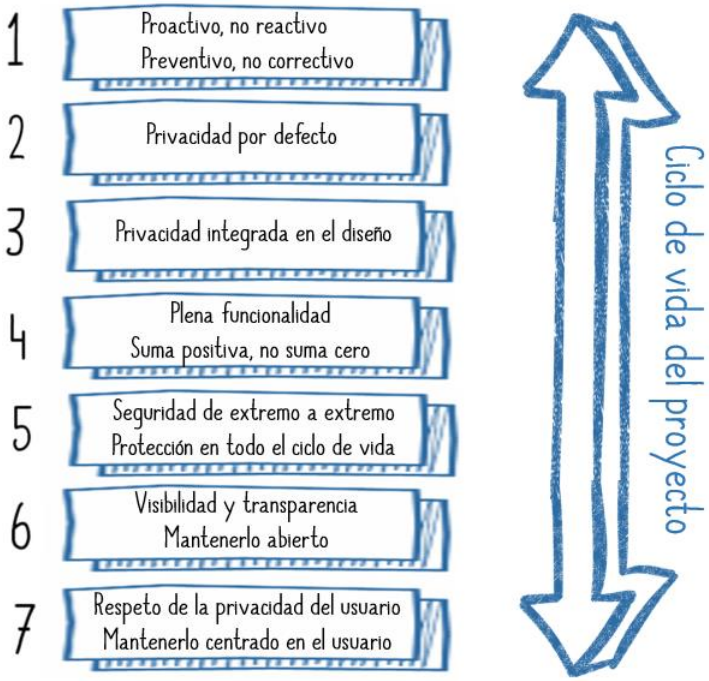
Formamos a nuestros empleados y mejoramos nuestros procesos internos.

- Aprendizaje sobre la revisión de “Security & Privacy” en “Projects & Contracts”.
- La plantilla de “Privacy Impact Assessment” se inicia automáticamente en nuestro software de gestión de la privacidad OneTrust@Roquette cuando es necesario.

Para saber mas: CNIL Metodología de la PIA, Edición de febrero de 2018 - https://www.cnil.fr/en/home.

Privacidad desde el diseño y por defecto

La **Privacidad desde el diseño** significa construir la privacidad dentro del diseño, el funcionamiento y la gestión de un sistema, proceso de negocio o especificación de diseño.



¿Qué es la Protección de datos desde el diseño?

La legislación de protección de datos contiene principios básicos para salvaguardar la privacidad de los titulares de los datos.

La protección de datos desde el diseño y por defecto ayuda a garantizar que los sistemas de información que utilizamos cumplan con estos principios de protección de datos, y que los sistemas salvaguarden los derechos de los titulares de los datos.

Consideramos que:

Roquette se basa en sistemas de información y bases de datos para realizar una serie de tareas operativas y administrativas. Una gran parte de esos sistemas de información tratan datos personales, por lo tanto, su pleno cumplimiento de la regulación es de suma importancia.

Las empresas que se toman en serio los problemas relacionados con la protección de datos generan confianza.

Por lo tanto, adoptar medidas fuertes de protección de datos puede ser una ventaja competitiva.

El compromiso de la dirección es crucial para tomar la decisión de aplicar los principios de uso de protección de datos desde el diseño en las adquisiciones de la organización y el desarrollo del software.

La dirección también debe asegurarse de proporcionar recursos suficientes para esta tarea.

Tener en cuenta la protección de datos durante todo el proceso de desarrollo es rentable y más eficiente que realizar cambios en un software existente.

Nuestras responsabilidades:

Según el RGPD, la protección de datos desde el diseño se ha convertido, por primera vez, en una obligación legal. Esto significará que la protección de datos y la privacidad deben integrarse en las especificaciones del diseño y la arquitectura de los sistemas y tecnologías de información y comunicación.

Como encargado de datos, Roquette debe cumplir con los requisitos que rigen la protección de datos desde el diseño durante el desarrollo del software y al encargar sistemas, soluciones y servicios.

Por consiguiente, los requisitos también deben incluirse al celebrar acuerdos con proveedores y al utilizar servicios de consultores (consulte nuestras normas para los subcontratistas).

Norma	Referencia Q-Docs	Referencia RGPD
• Seguridad, privacidad y protección de datos desde el diseño y por defecto	DDPG007EN Norma 3	Art. 25

Lista de comprobación:

- ☑ Revisar la Evaluación de impacto en la protección de datos (DPIA)
- ☑ Evitar, limitar o minimizar la necesidad de recopilar y tratar datos personales confidenciales
- ☑ Limitar y minimizar la exposición de las funcionalidades y los datos personales innecesarios en la interfaz de usuario
- ☑ Anonimizar o seudonimizar datos personales siempre que sea posible
- ☑ Todas las configuraciones orientadas a la privacidad deben estar activadas por defecto
- ☑ El rastreo de un sitio web a otro debe estar deshabilitado de forma predeterminada
- ☑ Retirar el consentimiento a través de un menú dentro del software. Tener en cuenta que la recopilación de datos personales debe cesar si se retira el consentimiento
- ☑ Las configuraciones deben presentarse en un menú donde el titular de los datos deba hacer una elección consciente para "cambiar" activamente a configuraciones menos orientadas a la privacidad
- ☑ El rastreo del dispositivo debe estar deshabilitado de forma predeterminada

Formamos a nuestros empleados y mejoramos nuestros procesos internos.

- Orientación en nuestra Comunidad “Red de protección de datos”.
- Metodologías: Revisión de la seguridad y el cumplimiento en los proyectos y contratos.
- Formación en Plataforma de RRHH.

Notificación de la violación de datos

¿Qué es una violación de los datos personales?

La **violación de los datos personales** implica una violación de la seguridad que conduce a la destrucción accidental o ilegal, pérdida, alteración, divulgación no autorizada o acceso a datos personales transmitidos, almacenados o tratados de otra manera.

*Esto significa que una violación es más que la mera **pérdida** de datos personales.*

Ejemplos:

- Pérdida de una base de datos de clientes
- Divulgación de la evaluación del desempeño de los empleados

Nuestras responsabilidades:

Tenemos que aplicar normas para tratar toda violación de los datos personales de tal manera que limitemos su impacto en los titulares de os datos y prevengamos que esto vuelva a suceder.

Normas	Referencia Q-Docs	Referencia RGPD
• Notificación de una violación de los datos personales al Responsable de la protección de datos.	DDPG008EN Norma 1	Art. 33
• Notificación de una violación de los datos personales a la autoridad de supervisión.	DDPG008EN Norma 2	
• Comunicación de una violación de los datos personales al titular de los datos.	DDPG008EN Norma 3	Art. 34

¿Con quién debemos ponernos en contacto en caso de Violación de los datos?

Por favor, póngase en contacto con el Responsable de la protección de datos en dpo@Roquette.com y también la línea de alerta confidencial de Roquette alert@Roquette.com.

¿Cuánto tiempo tenemos para informar de una violación?

Debemos informar de una violación notifícale a la Autoridad de supervisión sin demora indebida, pero a más tardar 72 horas después de haberla observado.

¿Qué violaciones necesitamos notificar a la autoridad de supervisión pertinente?

Solo tenemos que notificar una violación a la autoridad de supervisión pertinente si esta es susceptible de generar un riesgo para los derechos y libertades de las personas. Si no se le hace frente, es probable que dicha violación tenga un efecto perjudicial significativo en las personas. Por ejemplo:

- dar lugar a una discriminación;
- daño para la reputación;
- pérdidas financieras; o
- pérdida de confidencialidad o cualquier otra desventaja económica o social significativa.

Tenemos que evaluar esto caso por caso y debemos ser capaces de justificar nuestra decisión de informar a la autoridad de supervisión de una violación.

¿Cuándo tenemos que notificársela a las personas?

Si existe la probabilidad de que una violación genere un **alto riesgo** para los derechos y libertades de las personas, debemos notificársela a los titulares de los datos directamente y sin demora indebida.

El deber de notificar una violación a una persona no se aplica si:

- hemos adoptado las medidas técnicas y organizativas apropiadas, y estas se aplicaron a los datos personales afectados por la violación;
- hemos tomado medidas posteriores que garantizarán que ya no se materialice ningún alto riesgo para los derechos y libertades de las personas; o
- ello implicaría un esfuerzo desproporcionado.

Cuando la comunicación de una violación implique un esfuerzo desproporcionado, debemos poner la información a disposición de las personas de otra manera igualmente eficaz, como una comunicación pública.

¿Con quién debemos ponernos en contacto en caso de violación de datos?

Póngase en contacto con el **Responsable de Protección de Datos** en dpo@Roquette.com y/o notifique el incidente a través de nuestro formulario web "Alerta de privacidad".

Si necesita notificar una posible infracción de la normativa, puede ponerse en contacto con su interlocutor habitual o notificar un problema a través del dispositivo de alerta confidencial de Roquette: Speakup©.

Supervisión y revisión

Consideramos que:

Roquette se compromete a:

- ☑ garantizar una **supervisión** legal y tecnológica sobre el requisito de la protección de datos,
- ☑ **revisar** y **mejorar** nuestro Sistema de gestión de la protección de datos (SGPD)

para tener en cuenta las evoluciones normativas y tecnológicas, así como los condicionantes internos de los servicios. [DDPG009EN]

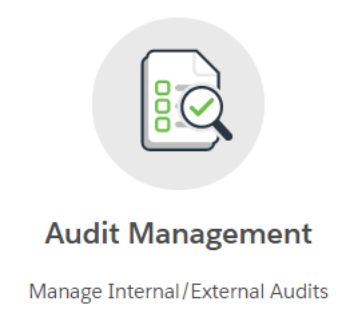
Nuestras responsabilidades:

Normas	Referencia Q-Docs	Referencia RGPD
• Garantizar una supervisión y revisión legal y tecnológica de la protección de los datos personales	DDPG009EN Norma 1	Buenas prácticas
• Supervisar periódicamente la aplicación del SGPD y de las directivas de protección de datos	DDPG009EN Norma 2	
• Revisar periódicamente la política de protección de datos personales y la documentación del SGDP	DDPG009EN Norma 3	

Formamos a nuestros empleados y mejoramos nuestros procesos internos.

OneTrust DataGuidance™ REGULATORY RESEARCH SOFTWARE

pdp Privacy & Data Protection News



Diseñar y dar soporte a nuestro Programa de privacidad

Software de investigación reglamentaria:

Utilizamos una plataforma que proporciona un conjunto de soluciones de privacidad diseñadas para ayudarnos a supervisar la evolución de la regulación, mitigar el riesgo y lograr el cumplimiento global:

- ☑ Seguimiento reglamentario
- ☑ Gráficos transfronterizos comparativos
- ☑ Notas de orientación
- ☑ Portal del RGPD
- ☑ Plantillas y listas de comprobación
- ☑ Consulta a un servicio de analistas
- ☑ Investigación legal

Auditoría y revisión del Sistema de gestión de protección de datos:

Realizamos auditorías internas para determinar si las entradas del SGPD son:

- ☑ conformes a los requisitos de esta Guía, la Política y la legislación o normativa aplicable;
- ☑ se aplican y mantienen de manera eficaz; y
- ☑ se realizan según lo esperado.

Realizamos una revisión de la gestión del SGDP para garantizar que su alcance siga siendo el adecuado y que se identifiquen mejoras en el proceso del SGDP.

Para ello, las entradas son:

- ☑ Objetivos, controles, procesos y procedimientos del SGDP;
- ☑ Resultados de auditorías y controles de cumplimiento anteriores;
- ☑ Comentarios de las partes interesadas;
- ☑ Técnicas, productos o procedimientos, que podrían utilizarse en la organización para mejorar el rendimiento y la eficacia del SGDP;
- ☑ Estado de las acciones preventivas y correctivas;
- ☑ Vulnerabilidades o amenazas no abordadas adecuadamente en la evaluación de riesgos previa;
- ☑ Resultados de las mediciones de eficacia;
- ☑ Acciones de seguimiento de revisiones de gestión previas;
- ☑ Cualquier cambio que pueda afectar al SGDP; y
- ☑ Recomendaciones de mejora.

Documentos de referencia

- [Código de conducta] Código de conducta del Grupo Roquette
- [GDPG001EN] Glosario de definiciones relativas a la protección de datos
- [MDPG001EN] Manual de protección de datos personales
- [DDPG001EN] Directiva sobre la cultura del respeto de la privacidad y la protección de datos
- [DDPG002EN] Directiva sobre la legalidad del tratamiento de los datos personales
- [DDPG003EN] Directiva sobre la evaluación de impacto en la privacidad
- [DDPG004EN] Directiva sobre el tratamiento de los datos sensibles
- [DDPG005EN] Directiva sobre los registros de las actividades de tratamiento
- [DDPG006EN] Directiva sobre el respeto de los derechos de las personas
- [DDPG007EN] Directiva sobre la seguridad de los datos personales
- [DDPG008EN] Directiva sobre la notificación de una violación de los datos personales
- [DDPG009EN] Directiva sobre la revisión del sistema de gestión de protección de datos
- [DSUG001EN] Directiva de protección de la información
- [DSUG006EN] Gestión de la Directiva de seguridad cibernética
- [DSUG016EN] Directiva sobre la seguridad de los contratistas

Bibliografía

[EU Charter] Carta de los Derechos fundamentales de la Unión Europea, 2010/C 83/02.

[RGPD] 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 dichos datos, y por el que se deroga la Directiva 95/46 / CE (Reglamento general de protección de datos).

[Ley sobre la PD] Ley francesa sobre protección de datos núm. 78-17 del 6 de enero de 1978, modificado 25.

[WP29 – Directrices] Directrices para identificar la autoridad de supervisión principal de un encargado o responsable | WP 244 rev.01 (5 de abril de 2017).

[WP29- Directrices] Directrices sobre la evaluación del impacto en la protección de datos (DPIA) y determinar si "es probable que el tratamiento genere un alto riesgo" a los efectos del Reglamento 2016/679 | WP 248 rev.01 (13 de octubre de 2017).

[WP29- Directrices] Directrices sobre la aplicación y fijación de multas administrativas a efectos del Reglamento 2016/679 | WP 253 (21 de octubre de 2017).

[WP29- Directrices] Directrices sobre la toma de decisiones y la elaboración de perfiles individuales automatizados a los efectos del Reglamento 2016/679 | WP 251 rev.01 (13 de febrero de 2018).

[WP29 – Directrices] Directrices sobre los responsables de la protección de datos ("DPO") | WP 243 rev.01 (5 de abril de 2017).

[WP29- Directrices] Directrices sobre transparencia en virtud del Reglamento 2016/679 | WP260 rev.01 (11 de abril de 2018).

[WP29- Directrices] Directrices sobre el consentimiento en virtud del Reglamento 2016/679 | WP259 rev.01 (11 de abril de 2018).

[EDPB – Dictamen] Dictamen 23/2018 sobre las propuestas de la Comisión sobre órdenes europeas de producción y conservación de pruebas electrónicas en materia penal (Art. 70.1.b) (26 de septiembre de 2018).

[EDPB – Dictamen] Dictamen 28/2018 sobre el proyecto de decisión de ejecución de la Comisión Europea sobre la protección adecuada de los datos personales en Japón (5 de diciembre de 2018).

[EDPB – Dictamen] Dictamen 14/2019 sobre el proyecto de Cláusulas contractuales estándar presentado por DK SA (artículo 28 (8) GDPR) (12 de julio de 2019).

[EDPB- Recomendación] Recomendación 01/2019 sobre el Proyecto de lista del Supervisor Europeo de Protección de datos sobre las operaciones de tratamiento sujetas al requisito de una evaluación de impacto en la protección de datos (Artículo 39 (4) del Reglamento (UE) 2018/1725) (10 de julio de 2019).

[Respuesta conjunta EDPB – EDPS] Respuesta conjunta del EPDB-SEPD al Comité LIBE sobre el impacto de la Ley de la nube de los EE. UU. En el marco legal europeo para la protección de los datos personales (anexo) (10 de julio de 2019)

[EDPB Dictamen] Dictamen 13/2019 sobre el Proyecto de lista de la Autoridad de supervisión competente de Francia con respecto a las operaciones de tratamiento exentas del requisito de una evaluación de impacto en la protección de datos (Artículo 35 (5) GDPR) (10 de julio de 2019).

Fuentes

- Commission Nationale de l'Informatique et des Libertés
  - https://www.cnil.fr/en/home
  - Septiembre de 2019
  - Licencia: CC-BY-ND 3.0 FR
- Information Commissioner's Office
  - https://ico.org.uk/
  - Septiembre de 2019
  - Licencia de la Open Government Licence
- Unión Europea
  - https://eur-lex.europa.eu
  - 1998-2019
- https://www.iso.org/home.html
- https://www.dataguidance.com/
- https://www.onetrust.com/
- https://www.corporatefiction.fr/
- https://pixabay.com/fr/service/license/

Estas fuentes se utilizan única y estrictamente con fines educativos, de aprendizaje y de concienciación.

Los actores mencionados no respaldan ni garantizan el contenido de este trabajo.

Los derechos de propiedad intelectual, incluidos los derechos de autor en sus materiales, siguen siendo de su propiedad.

La versión en inglés de esta guía es la referencia.
Las traducciones de este documento pueden estar sujetas a interpretación.
Primera edición: Septiembre de 2019
Publicado por ROQUETTE FRERES
Diseño editorial y gráficos: Oficina de cumplimiento
Fotografía: de uso libre

Todos los derechos reservados. Ninguna parte de este documento puede ser reproducida ni utilizada de ninguna forma ni por ningún medio, electrónico o mecánico, incluyendo fotocopias, escaneo, grabación o por sistemas de almacenamiento o recuperación de información, sin permiso expreso y por escrito solicitado a dpo@roquette.com.

Limitado únicamente uso interno solamente.

ROQUETTE

Offering the best of nature™