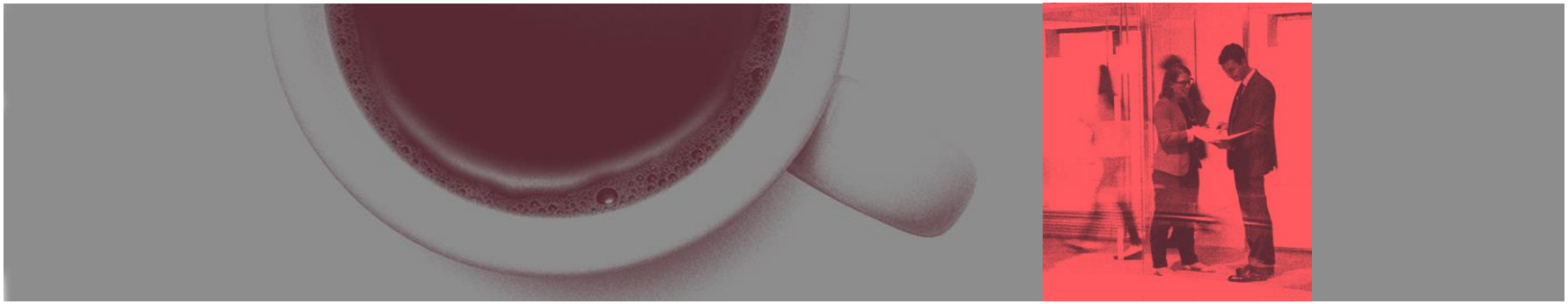
CUATRECASAS

1917-2017
100 AÑOS

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS EN EL ÁMBITO DE LOS SEGUROS



ALBERT AGUSTINOY
JORGE MONCLÚS

Barcelona, 14 de diciembre de 2017

Tres cuestiones fundamentales

- **CUÁNDO** → 25 de mayo de 2018

- **A QUIÉN** → A los responsables establecidos en la UE. Excepcionalmente, a responsables no establecidos en la UE.

- **ANTE QUIÉN** → Autoridad de control del establecimiento principal del responsable.

RESPONSABILIDAD PROACTIVA. PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

- El responsable debe establecer medidas apropiadas para **garantizar y poder demostrar** que el tratamiento de datos que realiza es **conforme con el RGPD**. Las medidas deben revisarse y actualizarse.

- **Protección de datos desde el diseño:** a la hora de establecer los medios para el tratamiento y durante el tratamiento, el responsable debe establecer medidas adecuadas para adecuarlo al RGPD y proteger los derechos de los interesados.

- **Protección de datos por defecto:** el responsable debe establecer medidas para garantizar que, por defecto, se traten únicamente los datos necesarios para los fines específicos del tratamiento. Esto afecta a la cantidad de datos recopilados, al alcance del tratamiento, al periodo de conservación y a la accesibilidad (por defecto, los datos no pueden hacerse accesibles a un número indeterminado de personas sin intervención de la persona).

BASES JURÍDICAS

- La licitud del tratamiento depende de la concurrencia de las bases jurídicas que establece el RGPD:
  - ✓ Consentimiento (explícito en algunos casos).
  - ✓ Ejecución de contrato o aplicación de medidas precontractuales.
  - ✓ Cumplimiento de obligación legal.
  - ✓ Protección de intereses vitales.
  - ✓ Cumplimiento de misión realizada en interés público o en ejercicio de poderes públicos.
  - ✓ Interés legítimo.
- Todas las bases jurídicas tienen la misma importancia.
- Debe informarse de la base jurídica a los interesados.
- **Prohibición general** de tratar datos sobre etnia o raza, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos (para identificación de personas), salud, vida sexual y orientación sexual.

DERECHO DE INFORMACIÓN

- En el momento de recogida/obtención de los datos debe informarse de:
  - Identidad y datos de contacto del responsable, representante y delegado.
  - Fines y base jurídica del tratamiento.
  - Destinatarios o categorías de destinatarios.
  - Transferencias a terceros países, indicando existencia o ausencia de decisión de adecuación de la Comisión, o referencia a las garantías adecuadas y forma de obtener una copia. 
  - Plazo de conservación o, si no es posible, criterios para determinar el plazo. 
  - Derechos de acceso, rectificación, supresión, oposición, limitación, portabilidad y, si hay consentimiento, derecho a retirarlo.
  - Derecho a presentar reclamación ante autoridad de control. 
  - Si existe obligación legal o contractual de facilitar los datos, o son necesarios para suscribir el contrato; si es obligatorio facilitar los datos y las consecuencias de no facilitarlos. 
  - Existencia de un mecanismo de decisión automatizado que comprenda la elaboración de perfiles indicando la lógica aplicada y la relevancia y consecuencias previstas del tratamiento. 
- Información por capas.

DELEGADO DE PROTECCIÓN DE DATOS

- Para compañías que realizan tratamiento de datos a **gran escala**.
- Posibilidad de designar un **único delegado** por grupo de empresas.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

- El **responsable** debe llevar un **registro de las actividades de tratamiento.**
- RAT & Documento de Seguridad: la extraña pareja.
- Por regla general, no aplicará a empresas de menos de 250 empleados.

NOTIFICACIÓN DE INFRACCIONES DE SEGURIDAD

- Como regla general, plazo máximo de 72 horas desde que tenga constancia.
- Notificación a los **interesados** cuando la violación tenga un alto riesgo para sus derechos y libertades

EVALUACIÓN DE IMPACTO

- Previamente a cualquier tratamiento que probablemente suponga un **alto riesgo** para los derechos y libertades de los interesados, el responsable debe evaluar el impacto de las operaciones de tratamiento.

- Obligatoria en los siguientes casos (ejemplos):

  - ✓ Evaluación sistemática y exhaustiva de aspectos personales basada en un tratamiento automatizado, a partir de la cual se toman decisiones que producen efectos jurídicos en relación con los particulares o les afectan significativamente.
  - ✓ Tratamiento a gran escala de categorías especiales de datos.
  - ✓ Observación sistemática a gran escala de una zona de acceso público.

- La autoridad de control puede determinar supuestos que requieran y no requieran evaluaciones de impacto. Deberá comunicarlo al CEPD.

- Si la evaluación de impacto indica que el tratamiento entraña un riesgo alto (a pesar de las medidas adoptadas), el responsable deberá consultar a la autoridad de control antes de proceder al tratamiento.

ENCARGO DE TRATAMIENTO (I)

- El responsable debe elegir un **encargado que ofrezca garantías suficientes**.
- Debe **regularse por contrato** (o acto jurídico equivalente), que deberá incluir:
  - ✓ Objeto, duración, naturaleza y finalidad del tratamiento, categorías de interesados y de datos personales, obligaciones y derechos del responsable y del encargado.
  - ✓ Obligaciones del encargado:
    - Garantizar el compromiso de confidencialidad de las personas con acceso a datos.
    - Implementar medidas de seguridad y ayudar al responsable a garantizar el cumplimiento de las obligaciones relativas a seguridad de los datos.
    - Asistir al responsable para atender los derechos de los interesados.
    - Poner a disposición del responsable información para probar el cumplimiento de sus obligaciones y permitir auditorías.
    - Informar inmediatamente al responsable si entiende que una instrucción vulnera la normativa de protección de datos.
    - Notificar violaciones seguridad.
    - Registro de actividades de tratamiento en nombre del responsable.

ENCARGO DE TRATAMIENTO (II) – sector asegurador

- Regulación en la **Ley 26/2006**, de 17 de julio, de mediación de seguros y reaseguros privados (art. 62):
  - Agentes de seguros exclusivos y operadores de banca-seguros exclusivos - **encargados del tratamiento** de la entidad aseguradora.
  - Agentes de seguros vinculados y operadores de banca-seguros vinculados - **encargados del tratamiento** de las entidades aseguradoras.
  - Corredores de seguros y de reaseguros - **responsables del tratamiento** respecto de los datos de las personas que acudan a ellos.
  - Auxiliares externos - **encargados del tratamiento** de los agentes o corredores de seguros con los que hubieran celebrado el correspondiente contrato mercantil.
- El **régimen actual seguiría vigente** con el RGPD, salvo modificación legislativa específica.
- Será preciso **actualizar los contratos** de agencia/encargo de tratamiento al nuevo RGPD.

MEDIDAS DE SEGURIDAD

- Las medidas de seguridad no están predeterminadas, sino que deben ser adecuadas al riesgo y tener en cuenta factores tales como el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento.

- Ejemplos: seudonimización; cifrado; medidas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; medidas para restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

- Necesidad de realizar auditorías ("verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento").

SANCIONES

- Sanciones económicas:
  - ✓ Hasta 10 millones de euros o hasta el 2% del volumen de negocios mundial total anual del ejercicio financiero anterior (el importe más elevado): obligaciones de responsable/encargado, de organismos de certificación y de autoridades de control.
  - ✓ Hasta 20 millones de euros o hasta el 4% del volumen de negocios (el importe más elevado): principios básicos, no atención de derechos, transferencias internacionales.
  - ✓ Hasta 20 millones de euros o hasta el 4% del volumen de negocios (el importe más elevado): Incumplimiento de resoluciones de autoridades de protección de datos.

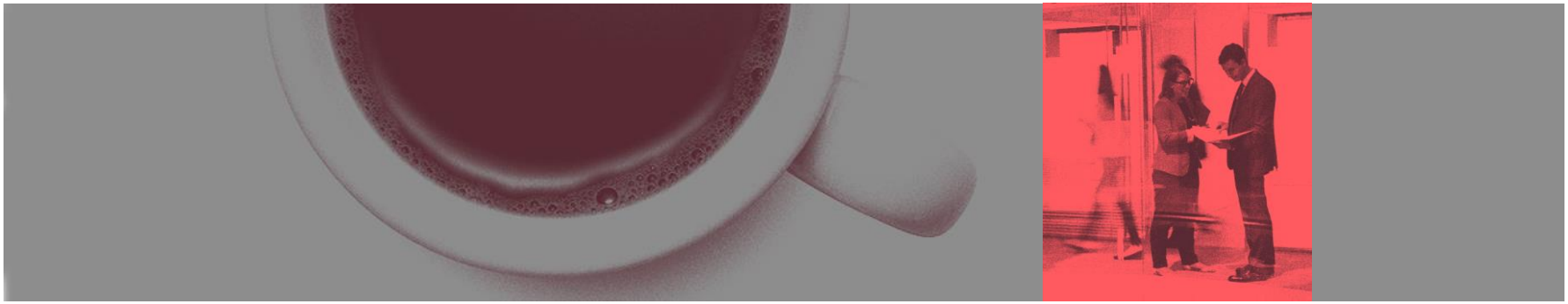
RECOMENDACIONES

- Elaborar el registro de actividades del tratamiento.
- Adaptar las cláusulas informativas.
- Revisar aquellos tratamientos basados en el consentimiento que puedan verse afectados por la derogación del consentimiento tácito.
- Preparar adendas a aquellos contratos de prestación de servicios que impliquen un encargo de tratamiento.
- Valorar si hay tratamientos que se prevean realizar a partir de mayo de 2018 que puedan requerir una evaluación de impacto.
- Elaborar políticas internas para la atención de derechos, la realización de evaluaciones de impacto, la notificación de violaciones de seguridad...
- Valorar la necesidad o conveniencia de nombrar un DPO. Elaborar un documento recogiendo sus funciones.
- … Llamar al abogado…

CUATRECASAS

1917-2017
100 AÑOS

MUCHAS GRACIAS



albert.agustinoy@cuatrecasas.com

jorge.monclus@cuatrecasas.com