Universidad de San Carlos de Guatemala
Facultad de ingeniería
Seminario de Sistemas 2
Sección A

Edgar Mauricio Gómez Flores
2011-14340
11/02/2025

General Data Protection Regulation(GDPR)

Es una regulación de la Union Europea que define como la información privada se puede usar dentro de la Union Europea y el Area Económica Europea(EEA) . Impone obligaciones a las organizaciones de cualquier parte del mundo si manejan o recolectan información relacionad a gente en la Union Europea. Establece un marco de trabajo para la recolección, procesamiento, almacenamiento y transferencia de información personal.

¿Cómo esta ley protege a los individuos sobre el uso de sus datos?

Principios de Protección de Datos

Esta ley define a la información personal como cualquier información que se relacione con un individuo que puede ser directa o indirectamente identificado y define siete principios de protección y responsabilidad de datos en el **articulo 5.1-2**

1. Licitud, lealtad y transparencia
2. Limitación de la finalidad
3. Minimizacion de datos
4. Exactitud
5. Limitación del plazo de conservación
6. Integridad y confidencialidad
7. Responsabilidad

Responsabilidad

Los controladores tienen que ser capaces de demostrar que estand cumpliendo con las normas, principios establecidos en GDPR. Formas de hacerlo

1. Designar responsabilidades de proteccion de datos al equipo
2. Mantener documentación detallada que explique que información se esta recolectando, como se usa, donde se guarda, que empleado es responsable de la información
3. Entrenar al staff e implementar medidas técnicas y organizacionales
4. Tener contratos de acuerdos de procesamiento de datos con entidades que se contraten para procesar los datos
5. Designar a un Data Protection Officer, aunque no todas las compañías necesitan uno.

Seguridad de datos

Se requiere “implementar medidas técnicas y organizacionales” . Medidas técnicas como requerir a los empleados 2FA(two-factor autenticaion) en las cuentas donde la información se este guardando en proveedores de nube que usen encriptación end-to-end.

Medidas organizacioales como entrenar al staff, agregar una política de privacidad de datos al manual de los empleados, limitar el acceso a solo empleados que necesiten los datos.

En caso de una fuga de datos, se tiene 72 horas para notificar a los afectados o se incurre en penalizaciones aunque este requerimiento puede no ser obligatorio dependiendo de las medidas tecnológicas de seguridad como la encriptación en la que un atacante no pueda leer la información debido a esta medida.

Proteccion de Datos por Diseño y por Defecto

Como se define en el **article 25** se tienen que considerar los principios de protección de datos en el diseño de cualquier producto y actividad.

Cuando Es Permitido Procesar Datos

No se deberia recolectar, guardar, vender información a menos que se pueda justificar que se pueda justificar con cualquiera de los siguientes motivos definidos en el **articulo 6**

1. El usuario dio permiso especifico y claro para usar su información, como aceptar emails de marketing
2. Cuando es necesario ejecutar el procesamiento de datos para prepararse para realizar un contracto que el usuario desea realizar, como realizar chequeos de identidad y solvencia antes de rentar una propiedad
3. Cuando se debe cumplir con una obligación legal, como cuando se recibe una orden judicial
4. Si es necesario para salvar la vida de una persona
5. Cuando se realiza una tarea de interés publico o para ayudar a cumplir la función de un oficial.
6. Cuando tienes un interés legitimo para hacerlo. Ya que es difícil definir un caso de uso acá se puede referir al "Information Commisioner's Office" del Reino Unido

Consentimiento

Las reglas que definen que se considera **consentimiento de un usuario** para procesar sus datos, una idea de lo que estas definen es:

1. El consentimiento debe de ser dado libremente, especifico, y claro(sin ambigüedad)
2. Solicitud de consentimiento deben de ser claramente distinguible de otros asuntos y deben ser presentados en lenguaje claro y conciso
3. El usuario puede retirar su consentimiento cuando desee y este cambio debe de ser procesada legítimamente
4. Niños menores de 13 años solo pueden dar su consentimiento con el permiso de sus padres
5. Se debe documentar la evidencia de consentimiento}

Data Protection Officer

No todas las compañis necesitan designar este rol a un empelado. Las tres condiciones bajo las cuales es requerido designar este rol:

1. Eres una autoridad publica diferente a una corte actuando en su capacidad judicial
2. Tus actividades clave requieren que monitorees a las personas sistemática y regularmente a gran escala
3. Procesas datos a gran escala de las categorías definidas en el **articulo 9** o datos relacionados a convictos criminales y ofensas definidas en el **articulo 10**

Derechos de la Privacidad de la Personas

La lista de **derechos de privacidad de los usuarios** buscan darle al usuario mas control sobre los datos que le brindan a las organizaciones. Garantizar estos derechos aseguran que una organizacion cumplen con GDPR. Los derechos de privacidad de los usuarios son:

1. Derecho a estar informados
2. Derecho al acceso
3. Derecho a la rectificación
4. Derecho a la eliminación
5. Derecho a restringir el procesamiento
6. Derecho a la portabilidad de datos
7. Derecho a objetar
8. Derechos en relación a toma de decisiones y profiling automatizados

¿Permite la ley solicitar a una empresa la eliminación completa de la información de una persona?

SI, como pudimos observar en los dato anteriores, el consentimiento puede ser retirado y también tiene derecho a la eliminación