Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Normativa de Ciberseguridad

UD04. Legislación y jurisprudencia en materia de protección de datos.
Tarea Online 04.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

Caso práctico

isftic. *Antena de Telecomunicaciones* (CC BY-NC-SA)

La compañía ACME S.A. se encarga de proveer servicios de telecomunicaciones enfocados en comunicaciones internacionales tanto a particulares como a empresas.

ACME tiene una cartera de 300.000 clientes en España a los que ofrece estos servicios y por los cuales cobra una tarifa media de 23,5 € mensuales.

ACME está presente en 32 países, y se aprovecha de esta situación para dar servicio a multinacionales. Durante el año 2022 ACME ha logrado adjudicarse el servicio de telecomunicaciones de todas las embajadas en España.

Uno de sus clientes multinacionales es una entidad bancaria, con un nivel de madurez en seguridad elevado, uno de los requisitos que establece es la certificación ISO27001 en los servicios de comunicaciones.

La sede central de ACME se encuentra en Madrid, fue abierta en el año 2020, sus oficinas cuentan con climatización inteligente, jardines en las azoteas para mejorar la climatización y aprovechar el agua de la lluvia para los riegos de sus zonas verdes y paneles solares para mejorar la eficiencia energética.

Además, parte de los terrenos de la organización, han sido convertidos en parques públicos que pueden ser utilizados por los residentes de la zona, y los accesos por carretera a la zona han sido acondicionados, mejorados y reasfaltados.

Dada su cartera de clientes, ACME es responsable de la información de su cartera de 300.000 clientes, de los cuales maneja diversos datos como pueden ser, datos identificativos, de residencia, bancarios, de tráfico de llamadas, etc.… con diferentes sensibilidades. Existen dos regulaciones cuyo objetivo es la protección de los datos personales de los individuales, la Regulación General de Protección de Datos (GDPR) y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPD- GDD).

¿Qué te pedimos que hagas?

Teniendo en cuenta la compañía descrita en el escenario anterior, da respuesta a las siguientes preguntas:

- ✓ **Apartado 1: Principios de protección de datos.**
  - ➢ Enumera 10 datos de carácter personal que trate ACME en la prestación de sus servicios.

    1. Nombre y apellidos.
    2. Dirección postal.
    3. Dirección de correo electrónico.
    4. Número de teléfono.
    5. Número de identificación fiscal, NIE, similares.
    6. Datos bancarios.
    7. Historial de facturación.
    8. Tráfico llamadas.
    9. Información de uso de servicios de telecomunicaciones.
    10. Información de ubicación geográfica.
    11. Dirección IP.
    12. IDs Cookies.

  - ➢ ¿Alguno de los datos enumerados es sensible?

    No. Ninguno de los datos listados está sujeto a las condiciones para que sean considerados como sensibles:

    - datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas,
    - la afiliación sindical,
    - datos genéticos, datos biométricos tratados únicamente para identificar un ser humano,
    - datos relativos a la salud,
    - datos relativos a la vida u orientación sexuales de una persona.

- ✓ **Apartado 2: Regulación General de Protección de Datos.**
  - ➢ ¿Bajo qué escenarios se podría legitimar ACME en el tratamiento de datos de sus clientes?

    1. El interesado da su consentimiento: El propietario de la información da su consentimiento para el tratamiento de sus datos con uno o varios fines específicos.
    2. Cumplimiento de obligaciones legales: El tratamiento se ejecuta en base a una obligación legal.
    3. Ejecución de contrato: El tratamiento es necesario para la ejecución de un contrato firmado entre propietario y responsable de los datos.
    4. Interés público: El tratamiento es necesario para alguna actividad de interés público (considerando como servicio de interés público el área de negocio de ACME).
    5. Intereses legítimos: El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

➢ Indica al menos un ejemplo de cada figura de tratamiento de datos.

1. **Propietario de los datos / Interesado:** Los clientes de ACME, ya sea una embajada o un particular, han facilitado sus datos personales para que se les puedan prestar sus servicios de telecomunicaciones.
2. **Responsable del tratamiento de datos o controlador:** Es la propia ACME, como prestadora del servicio contratado y decidiendo sobre el fin y los medios del tratamiento de los datos personales facilitados por sus clientes.
3. **Encargado del tratamiento o procesador:** ACME puede subcontratar una empresa para realizar la centralización de pagos, cobros y morosidad de sus clientes, que obtendrá acceso a los datos personales necesarios para llevar a cabo sus tareas.

➢ Indica tres actividades de tratamiento que estén llevadas a cabo por ACME.

1. **Gestión de clientes:** Los datos identificativos, contacto, bancarios o de facturación y cobros como apuntamos antes, son tratados para poder llevar a cabo la gestión de clientes (facturación, cobros, resolución de incidencias, etc.).
2. **Análisis de tráfico y uso de los servicios:** El tratamiento de los datos de tráfico de llamadas, los mensajes y el uso de los servicios para mejorar la calidad de los servicios prestados.
3. **Marketing y publicidad personalizada:** ACME pude utilizar datos de contacto y las distintas preferencias de los clientes para enviarles información sobre nuevos servicios, tarifas o promociones.

✓ **Apartado 3: Análisis de impacto en privacidad.**

➢ Realiza un análisis de impacto de las tres actividades de tratamiento descritas en el apartado anterior.

Realizamos una evaluación de impacto de la protección de datos (EIPD) a las tres actividades:

1. **Gestión de clientes:**
   - **Descripción sistemática de la actividad:** Se necesitan tratar y almacenar de forma segura (BD centralizada accesible solo por personal autorizado) los datos identificativos, bancarios, facturación y todos aquellos necesarios para la correcta gestión de los contratos con los clientes.
   - **Evaluación de la necesidad y proporcionalidad:** Se hace necesario el tratamiento de estos datos tanto por obligación legal y contractual, como por la correcta gestión y realización de los servicios contratados.
   - **Evaluación de riesgos:** Se presentan riesgos como los accesos no autorizados o la pérdida de datos personales, que pueden suponer un riesgo para la privacidad. También puede haber errores en el tratamiento.
   - **Medidas previstas:** Implementación de políticas y procedimientos para el control de acceso a datos. Encriptación de datos sensibles en la base de datos y monitorización de accesos a ella. Formación sobre protección de datos del personal involucrado.
2. **Análisis de tráfico y uso de los servicios:**
   - **Descripción sistemática de la actividad:** Para mejorar el servicio prestado, se realizan análisis sobre los patrones de comportamiento y uso de los servicios: Volumen de tráfico, duración, horario o destinos frecuentes de las llamadas.

- **Evaluación de la necesidad y proporcionalidad:** Al ser una mejora de calidad, se hace necesario el tratamiento de datos para poder identificar las áreas de mejora.
- **Evaluación de riesgos:** Pueden presentarse riesgos de privacidad en la detección de patrones o por errores en el tratamiento.
- **Medidas previstas:** Implementación de políticas y procedimientos para el control de acceso a datos. Formación sobre protección de datos del personal involucrado.

3. Marketing y publicidad personalizada:

- **Descripción sistemática de la actividad:** Se utilizan los datos obtenidos para el diseño de acciones de marketing y publicidad adaptada a perfiles personales.
- **Evaluación de la necesidad y proporcionalidad:** Mejora la calidad del servicio, al ajustar la oferta publicitaria y de servicios a las necesidades que se detectan en el cliente.
- **Evaluación de riesgos:** La publicidad personalizada puede suponer ciertos riesgos. Si es excesiva o inadecuada, podemos encontrar discriminación por razas, religión, nacionalidades… además de vulnerar el derecho a la privacidad. También pueden presentarse riesgos por falta de transparencia.
- **Medidas previstas:** Comenzar por generar una información clara y transparente sobre el tratamiento de sus datos para estas acciones, dando incluso la posibilidad de decisión acerca de la cantidad de publicidad a recibir, y buscando el correcto cumplimento de las normas de protección de datos y la no discriminación.