TOPCERTIFIER
www.topcertifier.com

METODOLOGÍA DEL SERVICIO GDPR

PROTECCIÓN DE DATOS GENERALES REGULACIÓN

TOPCERTIFIER
www.topcertifier.com

INTRODUCCIÓN A GDPR

Los requisitos del GDPR se aplican a cada estado miembro de la Unión Europea, con el objetivo de crear más protección consistente de los datos de los consumidores y los datos personales en todos los países de la UE. Algunas de las claves Los requisitos de privacidad y protección de datos del GDPR incluyen:

- Requerir el consentimiento de los sujetos para el procesamiento de datos
- Anonimizar los datos recopilados para proteger la privacidad
- Proporcionar notificaciones de violación de datos
- Manejar de forma segura la transferencia de datos a través de fronteras
- Exigir a determinadas empresas que nombren un responsable de protección de datos para supervisar el cumplimiento del GDPR

GDPR exige requisitos regulatorios para todas las empresas que manejan datos de ciudadanos de la UE para salvaguardar mejor el procesamiento y el movimiento de los datos personales de los ciudadanos.

PATADA INICIAL

La reunión inicial es una herramienta esencial para comunicar y planificar la ejecución del proyecto. con obstrucción mínima y para completar el proyecto dentro del tiempo y costo planificados. La agenda de la reunión inicial es:

- Discusión del plan del proyecto: Esto incluye la discusión sobre la rendición de cuentas y la responsabilidad de partes interesadas. hitos y entregables del proyecto
- Alcance de los servicios
- Requisitos legales y reglamentarios

CREACIÓN DEL EQUIPO CENTRAL

- Nombramiento del delegado de protección de datos (DPO)
- Nombramiento del comité interno GDPR / GRC (Riesgo de Gobernanza y Cumplimiento) (*Si es necesario)

GDPR FORMACIÓN DE CONCIENCIACIÓN

Se llevará a cabo una formación de concientización sobre el GDPR para los empleados de su organización. el entrenamiento La sesión tiene como objetivo ayudar a los empleados a adquirir conocimientos, comprender los conceptos del GDPR y alinearlos. procesos y prácticas para lograr y establecer, implementar, mantener y mejorar continuamente un entorno de trabajo del sistema basado en el cumplimiento. Cuando el personal ha sido capacitados pueden pensar, actuar y contribuir al logro de los objetivos.

TOPCERTIFIER
www.topcertifier.com

GDPR - IMPLEMENTACIÓN POR FASE

FASE I - ANÁLISIS DE BRECHAS

Durante esta fase llevamos a cabo un análisis de brechas para verificar qué parte de sus prácticas actuales son en línea con los requisitos. Sus prácticas actuales se verifican con las dos siguientes criterios de referencia,

- GDPR Requisitos
- Requisitos legales, reglamentarios y estatutarios Los resultados de este análisis se presentan en forma de Informe de análisis de brechas. este informe actúa como la lista de elementos de acción para el recordatorio del proyecto

FASE II - EVALUACIÓN DEL FLUJO DE INFORMACIÓN

En esta fase ayudamos en la identificación de fuentes de información, y el procesamiento infraestructura que involucra personal, tecnología e infraestructura física con respecto a GDPR

FASE III - EVALUACIÓN DE IMPACTO EN LA PRIVACIDAD DE LOS DATOS (DPIA)

Una Evaluación de Impacto de la Protección de Datos (DPIA) es un proceso mediante el cual posibles problemas de privacidad y Los riesgos se identifican y examinan desde la perspectiva de todas las partes interesadas. Esto permite que el organización para anticipar, abordar los impactos probables de nuevas iniciativas a través de medidas para minimizar/reducir los riesgos. Las EIPD están diseñadas para minimizar el riesgo de daño que puede ser causado por el uso/mal uso de información personal al abordar la protección de datos y Preocupaciones de privacidad en la etapa de diseño y desarrollo de un proyecto.

Ayudamos a desarrollar un procedimiento de EIPD y un Registro de EIPD coordinando con el departamento funcional cabeza para que beneficie a la Organización gestionando los riesgos, evitando daños a reputación, velando por el cumplimiento de las obligaciones legales y mejorando la relación con los grupos de interés.

FASE IV - ANÁLISIS DE TRANSFERENCIA SEGURA DE DATOS PERSONALES

Ayudamos a analizar qué datos personales se transfieren fuera de su empresa y cuando además también ayudamos en el diseño de las medidas de seguridad necesarias para proteger adecuadamente datos personales y también los datos personales que se transfieren fuera de la empresa

FASE V – ESTABLECIMIENTO DEL PROCESO PARA INCIDENTES DE VIOLACIÓN DE DATOS

Ayudamos a configurar los procesos para identificar y manejar las violaciones de datos personales. (Por ejemplo, datos procedimientos de notificación de incumplimiento) y también ayudar en el desarrollo de procedimientos sobre notificación de incidentes. mecanismo a la autoridad supervisora interesada

TOPCERTIFIER
www.topcertifier.com

FASE VI - SOPORTE DE DOCUMENTACIÓN
Ayudamos en la implementación de las medidas organizativas y técnicas necesarias para proteger la datos personales de los interesados y también ayuda en el diseño de la documentación relevante con políticas y procedimientos de control que garanticen que el GDPR esté bien integrado en el procesos organizacionales

RESPONSABLE DE PROTECCIÓN DE DATOS FORMACIÓN EN AUDITORÍA INTERNA

GDPR Se brindará capacitación de Auditor Interno (IA) al DPO. Esta capacitación equipará a tales personal para analizar la necesidad de IA, planificar y programar la IA, preparar listas de verificación de auditoría y realizar una AI y documentar e informar sus observaciones a la alta dirección

GDPR AUDITORÍA INTERNA

Nuestros expertos supervisarán la realización de la auditoría interna por parte de su DPO. Esta auditoría interna identificar las brechas aún existentes en el sistema y demostrar el nivel de preparación para enfrentar las auditoría de cumplimiento. Esta auditoría le da a la organización la oportunidad de identificar y rectificar todos los incumplimientos. conformidades antes de proceder a la auditoría de cumplimiento. La alta dirección es notificada de la hallazgos de la auditoría interna.

GDPR - ANÁLISIS DE LA CAUSA RAÍZ (RCA) Y ACCIONES CORRECTIVAS

Todas las no conformidades identificadas durante la auditoría interna, auditorías de clientes o de terceros, o de Registro de riesgos, registro DPIA, registros de incidentes, registros de respaldo de datos, informes de notificación de violación de datos, Evaluación de vulnerabilidad y prueba de penetración (VAPT), registros de retención de datos y cualquier otra fuente tienen que estar listados. RCA se realiza utilizando técnicas como los métodos de lluvia de ideas y espina de pescado. Se implementan la corrección óptima y las acciones correctivas y se evalúa la efectividad de dichas acciones. Las acciones se documentan y revisan a través de un Informe de acciones correctivas (CAR) del GDPR.

Nuestros expertos estarán presentes con su equipo para guiarle a través del proceso.

TOPCERTIFIER
www.topcertifier.com

GDPR REVISIÓN DE LA GESTIÓN REUNIÓN (MRM)

El MRM es una oportunidad para que todas las partes interesadas se reúnan en intervalos programados para revisar, discutir y planificar acciones sobre los siguientes puntos de la agenda,

- Informes EIPD
- Desviaciones en aspectos de cumplimiento
- Informes de actividades posteriores a la entrega
- Plan de acción para resolver cualquier elemento abierto
- Oportunidades de mejora y cambios necesarios en el sistema

GDPR AUDITORÍA DE CUMPLIMIENTO

Cuando los niveles de preparación hayan alcanzado niveles adecuados, el proceso de Cumplimiento comienza la certificación. Un auditor designado por el Organismo de Certificación (OC) verifica la preparación a través de una auditoría externa. Esto implica que el auditor revise las políticas, procesos, SOP, aspectos críticos. registros operativos y registros de IA y MRM. Cualquier desviación importante de las expectativas del banco central. Se le notificará en este punto para introducir las correcciones necesarias. Esto reduce las posibilidades de No Conformidades mayores durante la auditoría de certificación. TOPCertifier se pondrá en contacto con todos partes interesadas y supervisar la finalización sin problemas de la auditoría.

CONTINUACIÓN DEL CUMPLIMIENTO

TOPCertifier será parte del proceso de cumplimiento de su organización y lo asistirá periódicamente Intervalos con capacitaciones necesarias, soporte del sistema y pupaciones, auditorías internas y externas. y renovación periódica de su certificación de Cumplimiento.