Mapa de Riesgos

Con la finalidad de cumplir con el 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 estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Este documento permitirá hacer una identificación de los riesgos que un producto o servicio puede entrañar para la protección de datos de los afectados. La gestión de los riesgos detectados se llevará a cabo con la ayuda del Manual de Protección de Datos para el Responsable. Este manual ayudará al Delegado de Protección de Datos (DPO) a enfrentarse a los diferentes riesgos detectados y a adoptar las medidas adecuadas para su minimización o eliminación.

Cada apartado de este documento responderá a la revisión de uno o más riesgos y en el campo de observaciones encontraremos las medidas correctoras o de supervisiones detectadas durante el proceso, que servirán como guía para futuras actuaciones de nuestra empresa.

**Toma de datos**

RAZÓN SOCIAL: ${razon}

CIF: ${cif}

ACTIVIDAD: ${cnae}

DOMICILIO: ${domicilio}

TELÉFONO: ${tel}

MAIL: ${email}

FECHA: ${fecha}

PERSONA QUE REALIZA EL CUESTIONARIO: ${cuestionario}

REPRESENTANTE LEGAL **(indicar cargo**): ${replegal}

NIF/DNI: ${dni}

PERSONA/S DESIGNADAS COMO RESPONSABLE DE TRATAMIENTO (**indicar cargo**): ${cargo}

**Estudio de Riesgos**

# RIESGO 1: LEGITIMACIÓN DE LOS TRATAMIENTOS Y LAS CESIONES DE DATOS PERSONALES

|  |
| --- |
| PUNTO DE CONTROL |
| ¿Se cuenta con el consentimiento libre, específico, inequívoco e informado de los afectados para el tratamiento de sus datos personales? |
| En caso contrario, ¿Está autorizado por una ley? ¿Proceden los datos de fuentes accesibles al público? ¿Está asociado al ejercicio de un derecho fundamental (libertad de expresión, libertad de información, tutela judicial efectiva, libertad sindical, etc.)? |
| ¿Se informa de la finalidad a la que se destinarán los datos? |
| ¿Se han habilitado procedimientos para gestionar la revocación del consentimiento del afectado? |
| OBSERVACIONES:  ${preg1} |

**RIESGO 2: TRANSFERENCIAS INTERNACIONALES**

|  |
| --- |
| **PUNTO DE CONTROL** |
| ¿Se van a transferir datos personales fuera de España? |
| ¿Es el país de destino un miembro del Espacio Económico Europeo? |
| OBSERVACIONES:  ${preg2} |

# RIESGO 3: NOTIFICACIÓN DE LOS TRATAMIENTOS A LA AEPD

|  |
| --- |
| PUNTO DE CONTROL |
| ¿Se han seguido los pasos necesarios para notificar al Registro General de Protección de Datos de la AEPD los ficheros o tratamientos de datos personales? |
| OBSERVACIONES:  ${preg3} |

**RIESGO 4: TRANSPARENCIA DE LOS TRATAMIENTOS**

|  |
| --- |
| PUNTO DE CONTROL |
| ¿Los datos se recaban directamente de los afectados? |
| Si los datos no se recaban directamente de los afectados, ¿se informa a los mismos, en el plazo de tres meses desde el registro de los datos personales, de forma expresa e inequívoca de la existencia de un tratamiento de datos personales, de la identidad y dirección del responsable del tratamiento, de su finalidad, de los destinatarios de los datos y de la posibilidad de ejercer los derechos ARCO? |
| OBSERVACIONES:  ${preg4} |

# RIESGO 5: CALIDAD DE LOS DATOS

|  |
| --- |
| PUNTO DE CONTROL |
| ¿Se recogen solo los datos personales estrictamente necesarios para las finalidades de que se trate? |
| ¿Se recaban los datos de forma leal y transparente? |
| ¿Se usan los datos para finalidades distintas o incompatibles con las establecidas y comunicadas al afectado? |
| ¿Se contempla la posibilidad de cancelar los datos personales de oficio, cuando ya no sean necesarios para la finalidad o finalidades para las que se recogieron? |
| OBSERVACIONES:  ${preg5} |

**RIESGO 6: DATOS ESPECIALMENTE PROTEGIDOS**

|  |
| --- |
| PUNTO DE CONTROL |
| ¿Se tratan con datos especialmente protegidos de ideología, religión, creencias o afiliación  sindical ¿se cuenta con el consentimiento expreso y por escrito? |
| ¿Se tratan con datos especialmente protegidos de salud, vida sexual u origen racial o étnico,  ¿se cuenta con el consentimiento expreso? |
| En el caso de tratamientos de datos especialmente protegidos para la prestación o gestión de servicios sanitarios, ¿se garantiza adecuadamente el deber de secreto de todas las personas que tienen acceso a ellos? ¿Se limita el acceso a los datos de salud a los estrictamente necesarios para cada una de las diferentes funciones (sanitarias, administrativas, investigadoras, docentes, etc.) que se llevan a cabo? |
| OBSERVACIONES:  ${preg6} |

# RIESGO 7: DEBER DE SECRETO

|  |
| --- |
| PUNTO DE CONTROL |
| ¿El personal de la empresa está debidamente informado de la forma de tratar los datos de carácter personal? |
| ¿Queda alguna constancia de la información? |
| OBSERVACIONES:  ${preg7} |

**RIESGO 8: TRATAMIENTOS POR ENCARGO**

|  |
| --- |
| PUNTO DE CONTROL |
| En el caso de que se externalice algún proceso de la empresa, ¿La empresa subcontratada cumple con las exigencias legales de la agencia española de protección de datos? |
| ¿Se estipula que el encargado solo podrá tratar los datos personales conforme a las instrucciones del responsable y no los aplicará a fines distintos? |
| ¿Se estipula que los datos no serán comunicados a otras personas? |
| OBSERVACIONES:  ${preg8} |

# RIESGO 9: DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN (DERECHOS ARCO)

|  |
| --- |
| **PUNTO DE CONTROL** |
| ¿Existen procedimientos necesarios para el acceso, la rectificación, cancelación u oposición de los datos personales? |
| ¿Se han adoptado medidas para acreditar la representación en casos de incapacidad o minoría de edad? |
| ¿Se conservan los datos personales de tal forma que permitan el fácil y rápido ejercicio de los derechos? |
| OBSERVACIONES:  ${preg9} |

**OTRAS INDICACIONES:**

**${otros}**