PRIVACIDAD Y CORONAVIRUS: ASPECTOS ESENCIALES

JUAN FRANCISCO RODRÍGUEZ AYUSO

Dykinson, S.L.

Introducción

Capítulo Primero. Declaración constitucional del Estado de Alarma y efectos generales sobre la Privacidad

I. Estado de alarma en tiempos de alarma

II. Nociones previas fundamentales

1. Objeto y ámbito de aplicación de la normativa actual en materia de protección de datos personales

2. Conceptos, objetivos y subjetivos, implicados

2.1. Dato personal

2.2. Tratamiento

2.3. Responsable del tratamiento, encargado del tratamiento y destinatario

2.4. Datos de salud, genéticos y biométricos

III. Datos personales de salud: contorno, encaje e implicaciones legales

1. Tratamientos de datos de salud

2. Tratamientos de datos salud a gran escala

3. Tratamientos de datos de salud con fines de investigación científica

IV. Legitimación en el tratamiento de categorías especiales de datos de afectados y potencialmente afectados por el COVID-19

1. Consentimiento como base jurídica tradicional: el supuesto singular de los menores de edad

2. Obligaciones emanadas de normas con rango legal

3. Interés vital del paciente

4. Intereses perseguidos por las Administraciones Públicas

V. Publicidad y transparencia de los tratamientos con fines de prevención, cuidado y atención

1. Supuestos de obtención directa de información sensible por el responsable del tratamiento

2. Deber de terceros cesionarios

3. Deberes de secreto y confidencialidad

Capítulo Segundo. Sujetos implicados en el tratamiento de datos de salud en supuestos excepcionales de emergencia sanitaria

I. El papel de los prestadores de servicios, públicos y privados, como encargados del tratamiento

1. Diligencia en la elección: sólo los más aptos

2. Contenido contractual: cuestión de mínimos

II. La necesidad y conveniencia del Data Protection Officer ante la crisis del coronavirus

1. Nombramiento de la figura atendiendo a la naturaleza del sujeto responsable y a la sensibilidad del dato

1.1. Tratamiento de datos personales llevado a cabo por autoridades u organismos públicos, a excepción de los tribunales que actúen en ejercicio de su función judicial

1.2. Tratamiento llevado a cabo por responsables y encargados del tratamiento cuyas actividades principales consistan en operaciones de tratamiento que, atendiendo a su naturaleza, alcance o fines, exijan de una observación habitual y sistemática de interesados a gran escala

1.3. Tratamiento llevado a cabo por responsables y encargados del tratamiento cuyas actividades principales consistan en operaciones de tratamiento a gran escala de categorías especiales de datos personales o de datos personales relativos a condenas e infracciones penales

2. Posición dentro de la organización: imparcialidad como elemento esencial

3. Cometidos en términos de numerus apertus, reforzados en tiempos de emergencia sanitaria

III. Administraciones Públicas y empleadores privados como responsables y encargados del tratamiento: tratamientos de personal no identificado y supuestos específicos relacionados con el COVID-19

1. Prevención y control sin necesidad de identificación: ¿obligación o diligencia?, ¿reacción o accountability?

1.1. Principio de licitud, lealtad y transparencia

1.2. Principios de minimización de datos y de limitación del plazo de conservación

1.3. Principio de integridad y confidencialidad

1.4. Principio de responsabilidad proactiva

2. Geolocalización de las personas infectadas o en riesgo de infección

3. Tomas de temperatura en establecimientos abiertos al público

Capítulo Tercero. Integridad y Confidencialidad como principio técnico esencial en tiempos del COVID-19

I. Nuevo enfoque en materia de seguridad: del dato personal al riesgo en el tratamiento como elemento nuclear

1. Identificación de los riesgos

2. Evaluación de los riesgos

3. Tratamiento de los riesgos

4. Protección de datos desde el diseño y por defecto

II. Medidas de seguridad en el contexto del coronavirus

1. La seguridad de las Administraciones Públicas: Esquema Nacional de Seguridad en el ámbito de la protección de datos personales

2. Medidas de seguridad aplicables en el contexto del COVID-19

2.1. Gestión de personal empleado en la organización responsable del tratamiento

2.2. Gestión de incidencias en materia de seguridad de los datos personales

2.3. Control de acceso físico y a los recursos del sistema que contienen información sensible

2.4. Protección de información especial

2.5. Sistemas de identificación y autenticación de usuarios con acceso a datos de salud

2.6. Protección de los soportes en que se contiene la información

2.7. Protección de los equipos, fijos y portátiles, empleados por los usuarios para el tratamiento de datos personales

2.8. Comunicaciones sensibles seguras a través de la red

2.9. Figuras complementarias al delegado de protección de datos: el responsable de seguridad

2.10. Auditoría de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos

3. Evaluación de impacto relativa a la protección de datos y consulta previa a la autoridad de control

III. Confinamiento de los ciudadanos durante la epidemia: el teletrabajo

1. Controles técnicos, organizativos o procedimentales

2. Cómo proceder ante una brecha de seguridad

2.1. Notificación a la autoridad de control de violaciones de seguridad de datos personales tratados con motivo de la pandemia

2.2. Comunicación a los afectados

Bibliografía