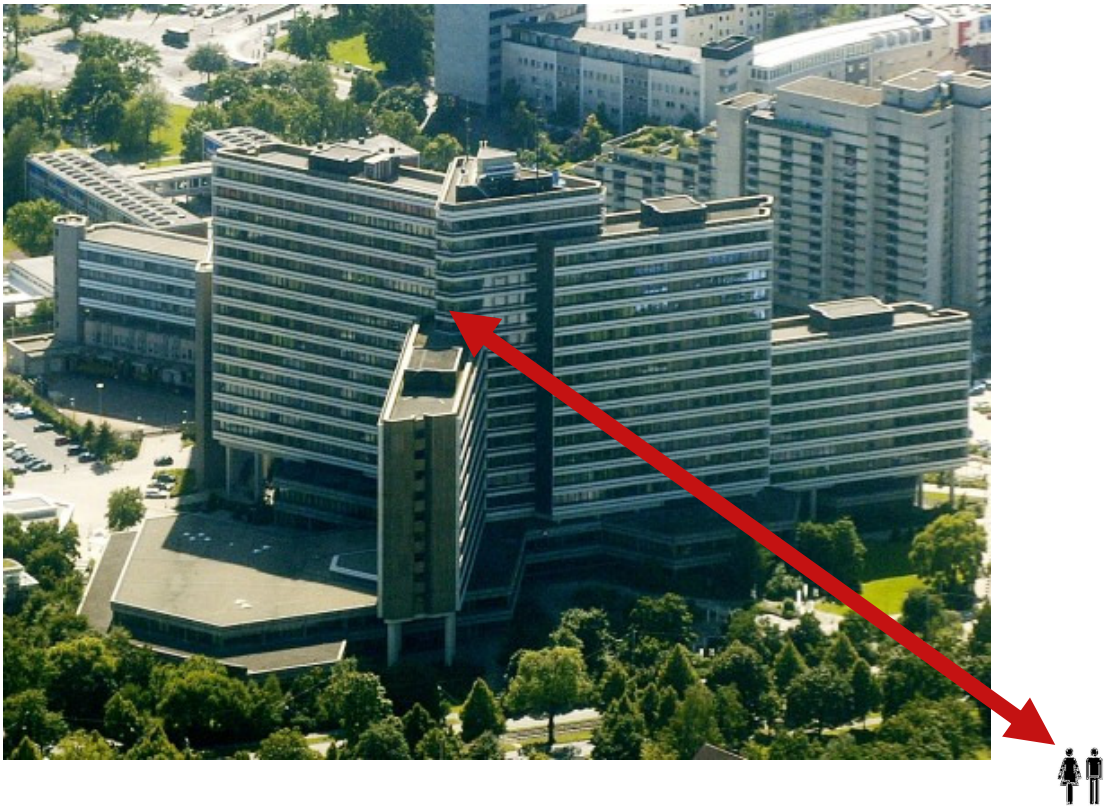
El Standard Datenschutzmodell(SDM)/ Modelo Standard de Protección de Datos Alemania

Ricardo Morte Ferrer
Martin Rost

Congreso Derecho TICs-SICARM 2014
Innovación, tecnología y gestión avanzada de la información administrativa
Implicaciones jurídicas del cambio de paradigma
Facultad de Derecho. Universidad de Murcia
23 y 24 de octubre de 2014

La Protección de Datos controla las relaciones asimétricas de poder en organizaciones y sujetos afectados



El 24 de Septiembre del 2010, el Consejo de Planificación TIC (IT-Planungsrat) alemán acordó y emitió una decisión sobre la Estrategia Nacional de Gobierno Electrónico (Nationale E-Government Strategie, NEGS) en la que el Gobierno Federal, los Länder y los Municipios decidieron de forma conjunta en qué dirección debía desarrollarse la Administración Electrónica mediante el uso de Internet. La mencionada Estrategia es la base para la colaboración entre las instancias antes

mencionadas, de forma que el desarrollo de la Administración Electrónica se produzca de forma coordinada, garantizando la interoperabilidad y la rentabilidad de ese desarrollo. Factores esenciales en esta Estrategia son la Protección de Datos, la Seguridad de los Datos y la posibilidad de controlar la Administación Electrónica, de forma que los ciudadanos la acepten y la utilicen de forma intensiva.

Las autoridades de Protección de Datos, en el mencionado marco, se ven obligadas a un alto grado de colaboración, de forma que se pueda garantizar un sistema uniforme de asesoría y auditoría de los modernos tratamientos automatizados de datos, de forma que la antes mencionada Estrategia sea desarrollada de acuerdo con las exigencias en materia de Protección de Datos. La existencia de procesos de tratamiento de datos que implican a diferentes Länder, como por ejemplo en temas de Seguridad Social o fiscales, requiere la existencia de un sistema de trabajo transparente y controlable en materia de Protección de Datos.

El Modelo Standard de Protección de Datos aquí presentado pretende ofrecer una posibilidad de trabajar de forma sistemática tanto en el ámbito público como en el privado, permitiendo un control eficiente de la relación entre las exigencias normativas, contractuales y organizativas y la aplicación efectiva en los procesos y sistemas TIC.

El tratamiento de datos personales por medio de sistemas informáticos debe ser valorado desde el punto de vista de la Protección de Datos en función de si tiene o no un fundamento jurídico adecuado. Cabe recordar que es aplicable la prohibición con excepción de autorización (Verbot mit Erlaubnisvorbehalt) del § 4 Abs. 1 BDSG (Ley Federal Alemana de Protección de Datos), o los artículos equivalentes de las leyes de los Länder. También debe controlarse si los datos personales son tratados con las medidas técnicas y organizativas adecuadas para la protección de los derechos del sujeto afectado.

El modelo aquí presentado intenta sistematizar las medidas en base a los objetivos de protección (Schutzziele). De esta forma, este modelo permite tanto que los responsables puedan planificar de forma adecuada esas medidas como que las autoridades de Protección de Datos puedan valorar de forma correcta los tratamientos y procesos afectados.

1.Objetivos del SDM

El tratamiento de datos personales por medios informáticos debe ser juzgado, de acuerdo con la normativa alemana, en función de si dispone de una base legal adecuada. Conviene recordar el principio de „Verbot mit Erlaubnisvorbehalt“ fijado en el § 4 Abs. 1 del Bundesdatenschutzgesetz (BDSG)[1] y en las normas de los Länder en materia de Protección de Datos, según el cual en principio cualquier tratamiento de datos está prohibido salvo que disponga de una base legal adecuada que haga posible su autorización. También debe controlarse si los datos serán tratados con las medidas técnicas y de organización adecuadas para permitir la protección de los derechos de la persona afectada.

1 Ley Federal de Protección de Datos

El SDM pretende sistematizar las medidas arriba mencionadas en base a los objetivos de protección (Schutzziele) que más adelante procederemos a explicar de forma detallada. De esta forma, este modelo permite tanto que los responsables puedan planificar y aplicar sus tratamientos de datos de forma sistemática y adecuada en materia de Protección de Datos como que las autoridades de Protección de Datos, utilizando esa misma sistemática, puedan valorar de forma transparente, comprensible y fundamentada esos tratamientos y sus componentes.

El punto de partida para el análisis es la finalidad fijada para el tratamiento de los datos, así como sus objetivos en relación con los procesos de negocio o administrativos para los que se utilizará ese tratamiento y sus bases legales. Este análisis de la base legal debe ser previo y será el que hará posible que en una fase posterior se valore la funcionalidad de los procesos incluidos en el tratamiento, el ámbito y volumen del mismo y la aplicación de las medidas de protección adecuadas al estado de la técnica.

2. Ámbito de aplicación del SDM

El principal ámbito de aplicación del SDM lo constituyen procesos utilizados en el tratamiento de datos personales. Estos procesos se caracterizan por tener un objetivo concreto, delimitado y legalmente justificado para el tratamiento del que forman parte, y por su relación con los procedimientos de negocio o administrativos orientados a ese mismo objetivo.

La normativa de Protección de Datos, tanto a nivel federal como de los Länder, exigen para cada tratamiento de datos personales la selección y aplicación de medidas técnicas y organizativas adecuadas al estado de la técnica y al nivel de seguridad requerido por los datos personales afectados. Dado que cualquier tratamiento de datos implica siempre diferentes procesos que deben ser claramente delimitables, desde el punto de vista de la normativa de Protección de Datos debe ser posible aplicar a cada uno de esos procesos medidas específicas. Si la normativa aplicable a un proceso exige la anonimización de los datos, esa anonimización será una medida técnica específica para ese proceso.

Aparte de las medidas específicas para cada proceso exigidas por la normativa, pueden existir también medidas sin relación directa con un proceso concreto. Ejemplos de este tipo de medidas pueden ser, la encriptación, medidas para garantizar la integridad, la autentificación de las comunicaciones y componentes técnicos, etc. Los responsables pueden implementar medidas específicas sin relación con los procesos concretos o con las exigencias legales. Este tipo de medidas también pueden ser sistematizadas y valoradas por medio del SDM.

3. Estructura del SDM

El SDM:

- incluye exigencias en materia de Protección de Datos de acuerdo con un catálogo de objetivos de protección,

- clasifica los procesos de los que se ocupa en base a los siguientes componentes: datos, sistemas informáticos y procedimientos,

- clasifica los datos en base a tres niveles de exigencia de protección,

- complementa el punto anterior con el análisis de las necesidades de protección de los sistemas informáticos y los procedimientos.

- y ofrece, en base a los puntos anteriores, un catalogo sistematizado de medidas standard de protección.

4. Exigencias en materia de Protección de Datos

Las exigencias presentadas a continuación, que están incluidas en toda la normativa alemana de Protección de Datos y cuyo cumplimiento es requisito previo para la legitimidad de un tratamiento de datos personales, están incluidas en el concepto de objetivos de protección:

- la finalidad de un tratamiento de datos personales,

- la limitación del tratamiento a lo indispensable para su finalidad,

- la atención a los derechos de los afectados, con especial atención los derechos de acceso, rectificación y cancelación de los datos,

- la transparencia como requisito previo para que las exigencias normativas sean fácilmente comprobables tanto para la organización responsable del tratamiento, como para las personas afectadas y para las autoridades de Protección de Datos,

- la seguridad de los datos en los componentes implicados en el tratamiento.

5. Los objetivos de protección básicos

Los objetivos de protección han jugado un papel básico en la organización de sistemas técnicos cuya seguridad debe ser garantizada desde finales de los años 80. Los objetivos de protección clásicos de la seguridad de los datos son:

- Disponibilidad, este objetivo refleja la exigencia de que los datos personales estén disponibles para ser utilizados de forma adecuada en el proceso para ellos previsto. Para ello deben ser accesibles para las personas previstas y se les deben poder aplicar los métodos previstos para su tratamiento, eso incluye, entre otras cosas, que los metodos sean aplicable al formato en el que los datos están disponibles. La disponibilidad incluye que los datos sean localizables, que los sistemas implicados los puedan presentar de forma adecuada y que esa presentación sea semánticamente comprensible.

- Integridad, en este caso el objetivo de protección resalta como exigencia que los procesos y sistemas informáticos sean capaces de mantener las características que son esenciales para la realización de las funciones imprescindibles para alcanzar la finalidad establecida y, al mismo tiempo, que los datos tratados permanezcan indemnes, completos y actuales. Posibles efectos secundarios deben ser evitados o tenidos en cuenta y tratados. Este objetivo de protección exige

que entre las exigencias y la realidad haya una garantía suficiente, tanto en los detalles técnicos como en lo que afecta al tratamiento en general y su ajuste a las finalidades establecidas.

- Confidencialidad, este objetivo de protección recoge como exigencia que nadie pueda acceder a los datos personales sin autorización. En ocasiones el acceso a los datos permite que el sujeto afectado sea identificado porque el contexto en el que los datos son almacenados permite sacar conclusiones sobre ese sujeto. Cuando nos referimos a personas no autorizadas, eso no significa que se trate necesariamente de terceros ajenos a la organización, que pueden actuar con intenciones criminales o de otro tipo, sino que puede tratarse también de empleados de servicios técnicos que para prestar esos servicios no precisan de acceso a los datos personales, o de personas activas en departamentos de la organización que no tienen ninguna relación con un determinado proceso o con el sujeto afectado.

Estos tres objetivos de protección han sido aceptados por los responsables por iniciativa propia, ya que los consideraban como necesarios para su propia protección sin que existiera una normativa legal que les obligara a aplicarlos. En un principio fueron formulados para su aplicación en el ámbito de la seguridad informática y describe exigencias para un operativo seguro, especialmente en lo que afecta a procesos en el marco de organizaciones y en relación con su negocio o administración. Esas organizaciones tienen que que proteger sus procesos, independientemente de que los posibles atacantes sean personas ajenas a ellas miembros de las mismas.

En función de la normativa aplicable, el nivel de exigencia en lo que afecta a estos objetivos de protección es variable. Por ejemplo, en el ámbito privado el objetivo de la disponibilidad se cumple siempre que los datos no sean destruidos ni se pierdan.

Aparte de los ya mencionados objetivos de protección originados en el campo de la seguridad informática, se han desarrollado otros objetivos cuyo interés se centra en la Protección de Datos basados en normativa existente en la materia y a partir de los cuales se pueden derivar medidas técnicas y organizativas. Desde el punto de vista de la normativa de Protección de Datos, las organizaciones deben proteger sus procesos de posibles ataques, siempre que esos procesos afecten a datos de carácter personal. Los objetivos de protección de la Protección de Datos precisan, en comparación con los objetivos de protección de la seguridad informática, de una grado de comprensión más amplio, ya que la Protección de Datos tiene en cuenta una perspectiva de protección adicional, al tener en cuenta los riesgos que las actividades de la organización en sí mismas pueden originar para el sujeto afectado, tanto en el ambito de sus procesos de negocio/administración como fuera de ellos. Desde el punto de vista metodológico eso significa que no sólo una persona debe demostrar ante una organización que es de confianza, sino que la organización debe ser capaz de demostrar frente a una persona que es de confianza. Por ese motivo es preciso establecer objetivos de protección que garanticen la protección de los sujetos afectados frente a diferentes tipos de organizaciones.

Estos objetivos de protección específicos de la Protección de Datos, cuya finalidad es la protección del sujeto afectado son:

- No encadenabilidad, refleja la exigencia de que los datos sólo sean tratados y valorados para la finalidad para la que fueron recogidos.

- Transparencia, requiere que, aunque en diferentes niveles, tanto el sujeto afectado, como el responsable de los sistemas y posibles autoridades de control puedan reconocer qué datos y para qué finalidad han sido recogidos y tratados en un proceso, que sistemas y procesos han sido utilizados, en qué dirección y para qué fines fluyen los datos y quien es el responsable legal de los datos y sistemas en las diferentes fases de un tratamiento de datos. La transferencia es imprescindible para el control y dirección de los datos, procesos y sistemas desde su inicio hasta su cancelación, y un requisito previo para que un tratamiento de datos sea legítimo y, en caso de necesidad, los sujetos afectados puedan otorgar su consentimiento.

La transparencia de un tratamiento de datos en su conjunto y de las partes implicadas puede permitir que especialmente los sujetos afectados y las autoridades de control puedan detectar posibles fallos y exigir que se lleven a cabo las modificaciones necesarias para suprimirlos.

- Capacidad de intervenir, exige que el sujeto afectado pueda ejercer de forma efectiva sus derechos ARCO en cualquier momento, y que el responsable está obligado a tomar las medidas necesarias para hacer efectivos esos derechos. Para alcanzar este objetivo debe ser posible modificar el tratamiento de datos en cualquier momento y en cualquiera de sus fases, desde la recogida de los datos hasta su cancelación.

En principio conjuntos o paquetes de datos son adecuados para ser utilizados para otros fines y para ser combinados con otros datos, posiblemente de acceso público. Cuanto mayores son esos paquetes de datos y cuanto más información aporten, mayor es el interés que despiertan. Desde el punto de vista legal, esas combinaciones sólo son aceptables en condiciones muy especiales y estrictamente fijadas. La normativa de Protección de Datos exige que el tratamiento sea separado en función de las finalidades y/o que los datos sean almacenados de forma separada en función de la finalidad para la que son tratados-

Al igual que sucede con los objetivos de protección clásicos, los de la Protección de Datos también están influenciados por la normativa que les es aplicable y por el ámbito en el que deben ser aplicados. Por ejemplo, en el ámbito privado la transparencia no es imprescindible en cada caso de uso de los datos en el campo de actuación de un responsable, salvo que ese uso suponga una modificación de los datos

6. Otros posibles objetivos de protección

Existen otros posibles objetivos de protección que han sido incluidos en normas de Protección de Datos de los Länder o en normas de ámbitos específicos, y que pueden derivarse de los objetivos mencionados en el punto anterior. Entre ellos cabe mencionar los siguientes:

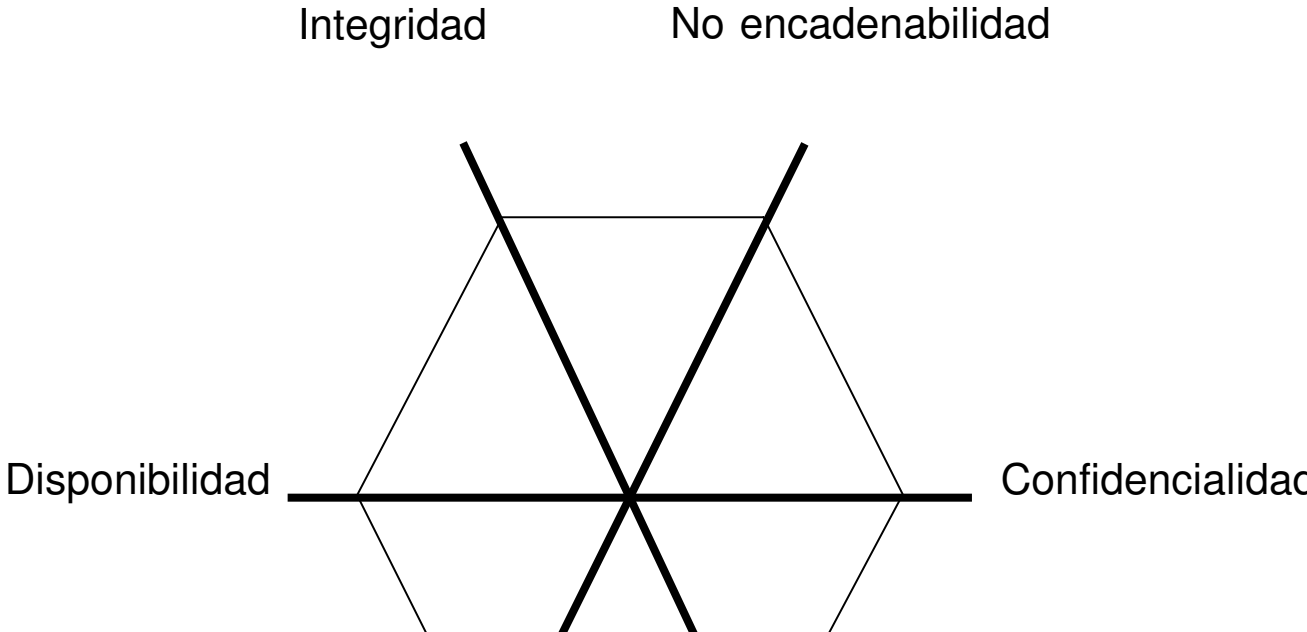
- Autenticidad, exige que se pueda fijar de forma garantizada el origen de los datos.

En función de ese origen, deberán guardarse determinadas informaciones y la relación de los datos con esas informaciones deberá ser protegida: en caso de que los datos hayan sido aportados por el sujeto afectado esas informaciones incluyen el procedimiento de recogida, el momento de la misma y eventualmente la identidad de quien ha efectuado la recogida; en caso de que los datos se hayan obtenido por una transferencia o por acceso a datos en posesión de terceros esas informaciones incluyen el momento de recogida, motivo de la misma y finalidad de la transferencia o acceso, así como la fuente de los datos; en caso de tratarse de una recogida para un cambio de finalidad deberá informarse del origen de los datos, de su nivel de control y se deberá otorgar acceso a su documentación.

Este objetivo de protección debe relacionarse con la garantía de la transparencia del tratamiento de datos. Este objetivo sólo puede alcanzarse garantizando la integridad de la conexión entre el conjunto de datos y su origen, de forma que se puede hablar de una „transparencia de integridad asegurada“.

- La posibilidad de auditar, refleja la exigencia de que sea posible demostar quien, cuando y qué datos personales ha tratado y de qué forma lo ha hecho. Este objetivo controla tanto tratamientos de modificación como usos y mero conocimiento de datos. Este objetivo también tiene como meta el garantizar la transparencia del tratamiento y sólo puede alcanzarse asegurando la integridad de la conexión entre el conjunto de datos y la justificación del tratamiento.

Los objetivos de protección como objetivos aplicables para la Protección de Dat para las organizaciones



7. Los objetivos de protección como medida de control

El punto de partida es el § 9 BDSG, que regula que responsable tanto públicos como privados, que ellos mismos o por encargo de terceros recojan, traten o usen datos personales deben tomar las medidas técnicas y organizativas necesarias para cumplir las exigencias del BDSG.

Los objetivos de protección se consideran incluidos entre las exigencias del BDSG y por eso se puede sancionar un incumplimiento de sus requisitos o se pueden ordenar las medidas previstas en el § 38 Abs. 5 Satz 1 BDSG para suprimir carencias en materia técnica u organizativa.

Aunque las exigencias fijadas en el BDSG responden a un contexto representado por centros de control o de servidores organizados de forma centralizada, que ya no responden a la realidad actual, los objetivos de protección permiten una aplicación de esa norma interpretándola de forma adecuada.

Pese a lo comentado arriba, ni el texto, ni el contexto ni la historia de la elaboración del § 9 BDSG ni su finalidad y sentido permiten una sustitución de las medidas previstas por los objetivos de protección. El legislador federal, a diferencia de los legisladores de los Länder no ha seguido las recomendaciones del AK Technik en el sentido de sustituir las medidas recogidas en el BDSG por objetivos de protección independientes de la técnica.

Por lo tanto, un control de las medidas técnicas y organizativas debe hacerse de acuerdo con lo previsto en el § 9 BDSG. En el SDM se presenta hasta que punto los objetivos de protección pueden ser incluidos/aplicados en esas medidas.

8. El anclaje de los objetivos de protección en el BDSG

- Disponibilidad, este objetivo de protección está incluido como medida en el n°7 del anexo al § 9 BDSG. El art.17.1.1 de la Directiva 95/46/CE exige medidas adecuadas para una protección contra borrados accidentales o ilegales o contra la pérdida ocasional de datos personales.

De lo expuesto no cabe extraer una obligación legal de la aplicación de este objetivo de protección.

- Integridad, en los anexos N° 1 a 6 del anexo al § 9 BDSG se incluyen medidas orientadas a garantizar la integridad. El art. 17.1 de la Directiva 95/46/CE exige medidas contra una modificación no autorizada de datos personales. Cabe mencionar la Sentencia del Tribunal Constitucional Alemán del 27.02.2008[2], que establece un „derecho fundamental a la confidencialidad e integridad de los sistemas informáticos".

Se puede extraer una obligación legal de lo expuesto en el § 20 bzw. § 35 Abs. 1 BDSG que establece una obligación de rectificación de efectuar la correspondiente notificación, la misma obligación se recoge en el Art. 12 de la Directiva 95/46/CE.

- Confidencialidad, en los anexos N° 1 a 6 del anexo al § 9 BDSG se incluyen medidas orientadas a garantizar la confidencialidad. El art. 17.1 de la Directiva 95/46/CE exige medidas adecuadas para la protección contra cesiones o accesos no autorizados.

En el § 5 BDSG y en el Art. 16 de la Directiva 95/46/CE se regulan el secreto de los datos y la confidencialidad.

- No encadenabilidad, este objetivo se puede alcanzar con medidas incluidas en el N° 8 del Anexo al § 9 BDSG.

En la normativa de Protección de Datos se fija la obligación de fijar la finalidad del tratamiento, especialmente en los §§ 4d Abs. 1, 4g Abs. 2 Satz 1, 4 e) así como en el § 28 Abs. 2 Satz 2 BDSG. En el caso de tratamientos de datos fundamentados en el consentimiento del afectado el § 4a Abs. 1 Satz 2 BDSG establece que se debe informar sobre la finalidad planeada.

La Directiva 95/46/CE regula en su Art. 6 b) que un tratamiento posterior debe ser compatible con la finalidad original.

- Transparencia, para los sujetos afectados se regulan derechos de información y notificación tanto en la Directiva 95/46/CE (Arts. 10, 11 y 12) como en el BDSG (§§ 4 Abs. 3, 4a Abs. 1 Satz 2, 33, 34).

Para el responsable, el § 4 Abs. 1 BDSG establece la obligación de tratar datos sólo en base a una regulación legal o al consentimiento del sujeto afectado. El responsable debe haber comprobado de forma previa si existe una autorización para el tratamiento. Exigencias especiales para la transparencia a nivel interno están reguladas en los §§ 4d Abs. 1, 4e y §§ 4g Abs. 2, 4e BDSG.

Las autoridades de control tiene derecho de información y de revisión de la documentación de acuerdo con los §§ 24 y 38 BDSG.

---

2 Entscheidung des Bundesverfassungsgerichts vom 27.2.2008 (BVerfG, 1 BvR 370/07)

Además, deben elaborarse listados de procesos que pueden ser solicitados por cualquier persona de acuerso con lo previsto en el § 38 Abs. 2 BDSG y § 4g Absatz 2 Satz 2 BDSG.

- Capacidad de intervenir, los procesos y tratamientos deben ser estructurados e implementados de forma que el afectado pueda ejercer sus derechos ARCO de forma efectiva.

9. Medidas básicas para la aplicación de los objetivos de protección

Para la elección y organización de las medidas de protección y para su valoración en el marco de actividades de control y auditoría se plantean numerosas cuestiones. En el marco de la seguridad de los sistemas informáticos existe un standard claro en materia de medidas técnicas y organizativas establecido por el BSI con su IT-Grundschutz[3], el SDM ofrece una base sistemática para el desarrollo de un standard equivalente en materia de Protección de Datos.

Para evitar caer en un listado interminable de medidas y variaciones de las mismas se deben identificar y describir características comunes a nivel general. Esas medidas de carácter general traspasan sus especificaciones a niveles inferiores de medidas de Protección de Datos con un campo de aplicación más reducido. Por medio de esta abstracción se consigue que algunas características de una medida sean aplicables en otro ámbito.

Medidas básicas de Protección de Datos y su legitimación legal establecen una posibilidad de puesta en común de conocimientos entre técnicos y juristas especializados en Protección de Datos.

A continuación presentaremos medidas básicas de Protección de Datos que han demostrado su utilidad en la práctica de control en esta materia a lo largo del tiempo y que permiten la puesta en práctica de requisitos de Protección de Datos y de los objetivos de protección.

Objetivo de protección no encadenabilidad

La puesta en práctica de este objetivo de protección se consigue cuando en un tratamiento de datos personales sólo se recogen, tratan, transfieren o comunican datos que cumplen la finalidad inicialmente fijada.

Número de la medida	**Descripción de la medida**	**Objetivo de la medida**	
Nichtv-G-001	Imposibilidad o establecimiento de obstáculos para la encadenabilidad de un proceso o de sus sistemas TIC, procesos datos con otro proceso y		Asegurar el cumplimiento de la finalidad

3 https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

	sus componentes, por medio de:	
Nichtv-G-001.1	Utilizar técnicas de programación que evitan o cierran interfaces entre procesos o sus componentes, a ser posible ya en la fase de desarrollo del Software.	
Nichtv-G-001.2	Medidas de regulación para prohibir la existencia de Backdoors, así como medidas de control de la calidad en materia de Compliance en el desarrollo del Software.	
Nichtv-G-001.3	Intervención el proceso, así como en la organización funcional de sus diferentes pasos.	
Nichtv-G-001.4	Control y elaboración de infórmenes sobre los componentes de red y de Hardware en materia de conectividad y elaboración de reglamentos internos.	
Nichtv-G-002	Separación técnica y organizativa de procesos y conjuntos de datos, así como de conjuntos de datos y sistemas TIC por medio de:	Garantizar la diferenciación de finalidades a nivel de □ Procesos □ Datos □ Sistemas TIC
Nichtv-G-002.1	Separación en base a límites en función de Organizaciones/Departamentos	Garantizar la diferenciación de finalidades dentro de la organización y entre diferentes unidades.
Nichtv-G-002.2	Separación por medio de conceptos de roles y derechos de acceso escalonados	Garantizar la diferenciación de finalidades en base funciones, grupos y personas autorizadas o no autorizadas
Nichtv-G-003	Imposibilidad o establecimiento de dificultades encadenamientos no justificados por la finalidad	Garantizar la diferenciación de la

	por medio de:	finalidad entre diferentes componentes del proceso o tratamiento
Nichtv-G-003.3	Utilización de pseudónimos	
Nichtv-G-003.4	Utilización de procedimientos de anonimización	
Nichtv-G-003.5	Utilización de credenciales anónimas	
Nichtv-G-003.6	Tratamiento de datos anonimizados	

Objetivo de protección transparencia

Número de la medida	**Descripción de la medida**	**Objetivo de la medida**	
Transp-G-001	Documentación de procesos en sus diferentes componentes □ Datos □ Flujos de datos □ Sistemas TIC □ Procesos de negocio generales □ Combinación con otros procesos (interfaces, protocolos, registros, transferencias) □ Contratos con empleados □ Contratos con prestadores de servicios □ Estructura de la organización, con división de funciones		□ Información sobre las estructuras técnicas y de procesos □ Permitir y grantizar el control de todas las estructuras □ Iimposibilitar o dificultar tratamientos ocultos o accesos no auotizados a los datos □ Distribución clara de responsabilididades y autorizaciones
Transp-G-002	Protocolizar los procesos de tratamiento		□ Garantizar el control de los

		procesos(empleado, programa, ordenador) quien ha trabajado en qué procesos y cuando □ Control de la relación entre la situación prevista y la realidad

La aplicación de las exigencias en materia de transparencia, que permiten un control de la relación entre la situación ideal o prevista y la real, es una condición previa para hacer posible la aplicación del resto de objetivos de protección.

Objetivo de Protección Capacidad de Intervenir

Número de la medida	**Descripción de la medida**	**Objetivo de la medida**
Interv-G-001	Actuaciones de la organización como responsable de los datos tratados: Establecer un Changemanagement que controle los siguientes puntos □ Deficiencias/alteraciones □ Gestión de posibles problemas □ Modificaciones en los procesos así como en las medidas de protección en materia de seguridad y de Protección de Datos	Hacer posible la intervención, de forma transparente y ajustada a la finalidad del tratamiento, en los diferentes procesos y tratamientos de datos
Interv-G-002	Actuaciones por parte de los afectados	Hacer posible la intervención, de forma transparente y ajustada a la finalidad del tratamiento por parte de los

		afectados a fin de poder ejercer de forma efectiva y comprobable sus derechos
Interv-G-002.1	El usuario tiene el control exclusivo sobre la entrega/recogida de sus datos: Establecimiento de un Single Point Of Contact (SPOC) para los afectados, que permita, de forma efectiva y controlable, las siguientes actuaciones en todo lo que afecta a datos de carácter personal: □ Acceso □ Modificación □ Borrado/Cancelación	
Interv-G-003	Actuaciones por parte de las Autoridades de Protección de Datos y del Data Protection Officer (DPO)	Hacer posible la intervención, de forma transparente y ajustada a la finalidad del tratamiento,en los procesos y tratamientos de datos por parte de diferentes instancias de control (autoridades, DPO, encargados de seguridad)

10. Niveles de Protección

En el establecimiento de los diferentes niveles de protección se tiene especialmente en cuenta la posible, de hecho frecuente, existencia de una relación asimétrica de poder entre organizaciones especialmente poderosas y los sujetos afectados.

El nivel de protección establecido afectará a los siguientes aspectos:

- Datos

- Sistemas

- Procesos

Se establecen tres niveles de protección:

a) Normal, los posibles daños son limitados y controlables para el afectado, quien podría tomar por sí mismo las medidas necesarias para corregirlos.

b) Alto, los posibles daños son considerables, por ejemplo debido a que los servicios a prestar por la organización son esenciales para la vida diaria del afectado y éste no podría solucionar los problemas por sí mismo.

c) Muy alto, los posibles daños suponen una amenaza inmediata de consecuencias posiblemente catastróficas para el afectado.

A continuación revisaremos las posibles situaciones de conflicto/daños para el afectado en base al BSI-Standard 100-2[4]. En concreto se tendrán en cuenta las posibles consecuencias para el individuo como tal, y no como posible miembro de la organización.

- Tratamiento ilegal de los datos.

- Limitación del derecho fundamental a la autodeterminación informativa.

- Posibles consecuencias para la reputación del afectado.

- Posibles perjuicios para la integridad del afectado.

- Posibles consecuencias de carácter económico.

- Posibles consecuencias para personas no directamente afectadas.

Nivel de protección „normal“	
Tratamiento ilegal de los datos	Un ejemplo sería un tratamiento transparente, aunque ilegal, llevado a cabo en interés del afectado, y con posibilidad de intervención por su parte.
Limitación del derecho fundamental a la autodeterminación informativa	Tratamiento de datos personales del afectado.
Consecuencias para la reputación del afectado	La reputación del afectado puede verse mínimamente afectada, el afectado podría tomas

4 https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30748/standard_1002_pdf.pdf

	medidas para corregir la situación.
Perjuicios para la integridad del afectado	No parece posible.
Consecuencias de carácter económico	Las consecuencias son tolerables o el responsable puede solventarlas.
Consecuencias para terceros	Puede tener consecuencias significativas a nivel social.

Nivel de protección „alto“	
Tratamiento ilegal de los datos	Tratamiento ilegal de los datos, que cabe esperar que no se produce en interés del afectado.
Limitación del derecho fundamental a la autodeterminación informativa	Tratamiento de datos de carácter personal del afectado que permiten el acceso a informaciones sobre su personalidad y posible comportamiento.
Consecuencias para la reputación del afectado	Cabe esperar consecuencias de este tipo, el afectado no podría solventarlas por si mismo y precisaría de ayuda externa.
Perjuicios para la integridad del afectado	Hay que considerar que estos perjuicios como posibles.
Consecuencias de carácter económico	Los posibles perjuicios son significativos, pero no peligrosos para su existencia.
Consecuencias para terceros	Cabe esperar significativas consecuencias a nivel social.

Nivel de protección „muy alto“	
Tratamiento ilegal de los datos	Tratamiento ilegal de datos, en contra de los intereses del afectado y con inmediatas consecuencias de carácter negativo.
Limitación del derecho fundamental a la autodeterminación informativa	Tratamiento de datos personales especialmente protegidos, que puede tener como consecuencia que el afectado sea controlado por la organización responsable del tratamiento y dependa de ella. Tratamiento de datos que normalmente deberían estar separados pero cuya combinación resulta interesante/rentable para la organización.
Consecuencias para la reputación del afectado	Existe la posibilidad de perjuicios graves, eventualmente peligrosos para su existencia.
Perjuicios para la integridad del afectado	Existe la posibilidad de perjuicios graves, incluso con peligro para la vida del afectado.
Consecuencias de carácter económico	Los perjuicios económicos son peligrosos para la existencia del afectado.
Consecuencias para terceros	Cabe esperar significativos efectos negativos a nivel social.

11. Control y asesoría en base al SDM

La finalidad esencial del SDM es organizar los procesos de control y asesoría de tratamientos de datos de carácter personal, de forma que sean ajustados a los requisitos de los objetivos de protección.

Para poder efectuar un control es preciso establecer cuales son las exigencias a cumplir. El siguiente paso es fijar de qué forma se debe fijar la situación real en el momento de llevar a cabo el control. La posibilidad de controlar de forma adecuada radica en establecer correctamente la relación entre las exigencias y la realidad. La capacidad de establecer esa relación entre la normativa legal las funciones técnicas y organizativas, es una condición sine qua non para que el DPO o las autoridades de Protección de Datos puedan decidir si los procesos de una organización son conformes a la normativa vigente y si las medidas técnicas y organizativas adoptadas cumplen las exigencias fijadas por esa normativa.

11.1 Establecimiento de las exigencias en base al SDM

El SDM se fija como objetivo el expresar los aspectos esenciales de la normativa de Protección de Datos por medio de los objetivos de protección. Cada uno de los objetivos de protección dispone de un catálogo de medidas de protección tanto técnicas como regulativas. Por ejemplo, a fin de cumplir con la exigencia de informar al afectado sobre qué datos se tratan, se manifiesta esa exigencia por medio del objetivo de protección „transparencia“, que se aplica por medio de dos grandes paquetes de medidas: la documentación de los diferentes volúmenes de datos, sistemas y procesos TIC, así como la protocolización de las diferentes actividades efectuadas por personas o sistemas TIC.

En los mencionados paquetes de medidas „Documentación y Protocolización“ se incluyen concretas exigencias normativas, como la exigencia de disponer de un listado de procesos y qué aspectos concretos se deben incluir. El grado exacto de cumplimiento de la normativa depende en gran medida del nivel de protección establecido para el tratamiento en concreto. Ese nivel de protección se extrae de un análisis de riesgos, que puede ser exigido por la normativa vigente o por códigos de buenas prácticas. El nivel de protección regula la calidad que deben reflejar las medidas de protección a aplicar, en el caso aquí comentado en que medida y con qué precisión se debe documentar y protocolizar. En lo que afecta a la protocolización, para un nivel de protección „alto“ se exigiría que los protocolos que controlan las actividades del administrador de sistemas deben estar fuera de su alcance. Junto con las medidas formuladas por los otros objetivos de protección y la información sobre los niveles de protección aplicables al proceso en cuestión, se establece un amplio abanico de medidas de protección que cabe que esperar que un controlador/auditor de Protección de Datos valore, refleje y/o aplique en sus procedimientos de control/auditoria.

11.2 Exposición de la situación real

Un controlador/auditor debe comprobar y documentar la situación a nivel legal, técnico y organizativo por medio de un inventario, comprobar si ya existe un documento de ese tipo o exigir que se elabore. En ese inventario se deben incluir la información referente la existencia de una justificación para la existencia del tratamiento de datos, los contratos con diferentes prestadores de servicios (especialmente con encargados de tratamiento), el organigrama de la organización y la distribución de funciones y responsabilidades en la misma. La finalidad de este inventario reside en

la posibilidad de controlar de forma adecuada el tratamiento de datos, así como al responsable del mismo. En la documentación se deben incluir tanto los aspectos legales como los temas técnicos y organizativos implicados en el proceso. Estos dos últimos puntos suponen incluir grandes cantidades de información, desde los diferentes sistemas operativos, bases de datos y el nivel de actualización de los mismos. Esta información, que sólo hace referencia a una parte del inventario, supondría en una pequeña organización con 50 ordenadores la recopilación de varios cientos de cualidades a tener en cuenta. En una organización de tamaño medio se pueden recopilar hasta 3000 cualidades referentes a los diferentes procesos implicados. Los objetivos de protección del SDM permiten centrarse en la presentación de las cualidades de procesos y sistemas relevantes en materia de Protección de Datos. Si, como ya hemos comentado, para garantizar la transparencia se recurre a la documentación y protocolización, el SDM establece de forma clara que para garantizar la disponibilidad se debe recurrir a medidas de copias de seguridad (Backup). En la medida que se prioriza la recopilación de cualidades del sistema y de reglas que están en relación directa con la controlabilidad de la calidad de las medidas de Backup utilizadas por la organización. También en esta materia cabe esperar con un elevado numero de cualidades a documentar, un número que irá aumentando con cada uno de los pasos a realizar con los diferentes objetivos de protección, por ejemplo: para garantizar la confidencialidad de los sistemas de Backup se recurrirá a la encriptación de los datos. El objetivo del inventario de las cualidades operativas de los procesos de una organización reside en la elaboración de un catálogo que refleje la situación real de la organización controlada/auditada. De esta forma se puede establecer una relación entre las medidas aplicadas actualmente y las medidas exigidas en el catálogo de medidas del SDM. Una vez establecida esa relación se puede proceder a iniciar el control.

11.3 El procedimiento de control

Un procedimiento de control consiste en comparar las medidas exigidas con las aplicadas actualmente,a efectos de fijar las coincidencias y divergencias existentes. El proceso de control consiste en proceder a valorar las divergencias encontradas. La valoración intentará establecer hasta qué punto las divergencias encontradas suponen un incumplimiento de la normativa vigente. Para poder aclarar esa cuestión, esencialmente legal, es imprescindible tener siempre presente la relación entre la mencionada normativa y los aspectos técnicos.

En la práctica habitual de control y auditoría es relativamente fácil comprobar qué exigencias no se cumplen, pura y simplemente porque las medidas previstas no han sido implementadas. En este caso el SDM permite al controlador establecer la relación entre las medidas no implementadas y las exigencias normativas. Algo más complicada es la situación planteada cuando la organización que está siendo controlada ha escogido una medida diferente de la prevista en el catálogo de referencia. La medida escogida podría ser valorada como adecuada en general, pero no aplicableen el caso concreto por no ser ajustada al nivel de protección exigido. Podría ser que la organización pretenda mantener la medida escogida anteriormente por considerarla equivalente a la recomendada en el catálogo de referencia. En este caso, el SDM ayuda al controlador a demostrar si la medida escogida por la organización es realmente equivalente a la de referencia. Si se confirmara que la medida escogida es suficiente y adecuada, se podría valorar el incluirla en el

catálogo de referencia como aceptada por ser „funcionalmente equivalente“. Hay que tener presente que la tecnología se encuentra en permanente desarrollo, por ello cabe preguntarse si esa medida sólo será aceptada en un Land o si será posible que se llegue a un acuerdo entre todas las autoridades de Protección de Datos en Alemania. Por ello se ha incluido en el SDM un procedimiento para introducir de forma acordada modificaciones en el catálogo de medidas de referencia o en otros aspectos del modelo,

Cuando la comparación entre las exigencias y la situación real realizada en base al SDM finaliza, se pueden empezar a mostrar las directrices de un modelo de gestión de Protección de Datos (Datenschutzmanagementsystem, DSMS). De forma análoga a la de los modelos de gestión de la seguridad TIC (IT Sicherheitsmanagementsystems, ISMS), se recurriría al ciclo PDCA[5] para una mejora continua del DSMS. Referente al ISMS, hay que recordar que entre las funciones de un DSMS se encuentra la de comprobar si las medidas de seguridad TIC son compatibles con las exigencias normativas en materia de Protección de Datos.

Bibliografía

Bock, K. / Rost, M. / (2011). Privacy by Design and the New Protection Goals - Principles, Goals, and Requirements. Retrieved March, 31st, 2013 from http://www.maroki.de/pub/privacy/BockRost_PbD_DPG_en_v1f.html

Probst, T. (2012). Generische Schutzmaßnahmen für Datenschutz-Schutzziele; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 439-444

Rost, Martin, 2012: *Standardisierte Datenschutzmodellierung*; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 433-438. http://www.maroki.de/pub/privacy/2012-06-DuD-SDM.html

Rost, M. (2012). Faire, beherrschbare und sichere Verfahren, in: Kersten, Heinrich (Hrsg).; Peters, Falk (Hrsg.); Wolfenstetter, Klaus-Dieter (Hrsg.), 2012: Innovativer Datenschutz, Berlin: Duncker & Humblot

Kirsten Bock, Martin Rost y Ricardo Morte Ferrer, (2012) http://www.redseguridad.com/opinion/articulos/evaluacion-pia-desde-el-punto-de-vista-del-sdm

Rost, Martin, 2013: *Datenschutzmanagementsystem*; in: DuD - Datenschutz und Datensicherheit, 37. Jahrgang, Heft 5: 295-300.

http://www.maroki.de/pub/privacy/2013-05_DuD-DSMS.html

Data Protection Management System - A future organizational approach to handle growing quantities of data? (in English)

5 https://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming

In: "A decade of transformations. Proceedings of the 10th International Conference on Internet, Law & Politics", Cerrillo-i-Martínez / Peguera / Peña-López / Vilasau Solana (Ed.), UOC-Huygens Editorial (Pub.), Barcelona 2014
Authors: Philipp E. Fischer, Ricardo Morte Ferrer
ISBN 978-84-697-0826-2, p. 343 - 356
Presented in Spanish at IDP Conference, Barcelona, 03-04/07/2014