ARBONIA

Directriz sobre el trato de los datos (directriz de protección de datos)

16. de junio de 2020

ARBONIA

ÍNDICE

ARBONIA

1 FINALIDAD Y OBJETIVO

Para el cumplimiento de obligaciones legales y contractuales es indispensable recopilar y procesar datos personales. Para ello, es obligatorio respetar las disposiciones de protección de datos vigentes en los países respectivos. La presente directiva indica cómo Arbonia AG y las sociedades del consorcio (en lo sucesivo "Arbonia" en general, o una empresa del consorcio individual, en lo sucesivo "empresa del consorcio") realizan el tratamiento de los datos personales. Las disposiciones fijadas se consideran los estándares mínimos. Si la ley de protección de datos local prevé disposiciones más estrictas, se deben respetar. También se deben respetar las eventuales disposiciones locales para la aplicación de la presente directriz.

La finalidad de esta directriz relativa al tratamiento de los datos ("directriz de protección de datos") es la determinación, la aplicación, el mantenimiento y la mejora continua del cumplimiento de la protección de datos por parte de Arbonia, según los requisitos del Reglamento General de Protección de Datos de la Unión Europea 2016/679 (el **RGPD**) y de todas las demás leyes locales vigentes de protección de datos (en conjunto las **leyes de protección de datos aplicables**).

El incumplimiento de las leyes de protección de datos aplicables expone a Arbonia al riesgo de daños a la reputación y multas delicadas (p. ej. de hasta un 4 % del volumen de negocios mundial en el marco del RGPD). Además, puede exponer a nuestros clientes y empleados a determinados riesgos relativos a la protección de datos, como una usurpación de identidad o pérdidas financieras. El cumplimiento de la normativa sobre protección de datos vigente nos ayuda a mantener la confianza en la organización de Arbonia y a garantizar que las operaciones comerciales tengan éxito.

El objetivo de esta directiva de protección de datos es facilitar el marco para dicho cumplimiento de la protección de datos dentro de Arbonia. Este documento pretende, en particular, aplicar los principios básicos para el tratamiento de datos personales (los **principios de protección de datos**) que se facilitan en el apartado 6 y de los que son responsables las empresas de Arbonia si estas actúan como responsables en el marco del RGPD, regula la necesidad de medidas técnicas y organizativas adecuadas y la notificación de incidentes de protección de datos como estándar mínimo para todas las empresas de Arbonia y se aplica a todos los empleados de Arbonia, así como a los miembros del Consejo de administración de Arbonia AG.

Además, proporciona un marco para otros requisitos que se aplican al responsable y al encargado del tratamiento en el marco del RGPD (o leyes de protección de datos aplicables similares), como se describe en el apartado 7.

2 DISPOSICIONES DE TÉRMINOS Y DEFINICIONES

Para el fin de esta directriz de protección de datos se aplican las siguientes disposiciones de términos y definiciones:

Datos anónimos significa que la identidad personal nunca puede ser rastreada o que la identidad personal solamente se podría rastrear con un esfuerzo de tiempo, costes y trabajo desmesurado.

Leyes de protección de datos aplicables hace referencia al Reglamento General de Protección de Datos de la Unión Europea 2016/679 (el **RGPD**) o a todas las demás leyes nacionales de protección de datos aplicables que incluyen disposiciones similares.

Propietario del proceso empresarial hace referencia a una persona natural que se considera responsable en el marco de esta directriz de protección de datos y que es responsable del tratamiento de datos personales y de la correspondiente aplicación informática.

Consentimiento hace referencia al consentimiento del interesado, es decir cada manifestación de voluntad concedida de forma inequívoca voluntariamente para un caso determinado, de manera informada y en forma de una declaración o de otra acción confirmatoria unívoca con la que la persona da a entender que está de acuerdo con el tratamiento de sus datos personales.

Responsable hace referencia a una persona jurídica o natural, autoridad, agencia u otra entidad que, sola o junto con otras, estipula las finalidades y los medios del tratamiento de los datos personales.

Incidente de seguridad de datos hace referencia a un acontecimiento en el que existe la sospecha justificada de que se registran, recopilan, modifican, copian, transmiten y usan datos personales de forma indebida. Esto puede hacer referencia a acciones de terceros o de empleados.

Interesado hace referencia a una persona natural identificada o identificable. Una persona natural identificable es una persona que se puede identificar directa o indirectamente, en particular mediante la asignación a un identificador, como un nombre, un número de identificación, datos de ubicación, un identificador en línea o una o varias características especiales que son la expresión de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de esta persona natural.

El **encargado del tratamiento** es una persona natural o jurídica, una autoridad, una institución u otra entidad que realiza el tratamiento de los datos personales por encargo del responsable.

Directorio de procedimientos de tratamiento hace referencia a un registro acerca del tratamiento de datos bajo la responsabilidad del responsable. Este directorio contiene todos los datos siguientes: (i) Nombre y datos de contacto del responsable y, si procede, del responsable general, del representante del responsable y del coordinador de protección de datos local; (ii) los fines del tratamiento; (iii) una descripción de las categorías de interesados y la categoría de los datos personales; (iv) las categorías de destinatarios cuyos datos personales se divulgan o se han divulgado, incluyendo destinatarios en terceros países; (v) si procede, la transferencia de datos personales a terceros países, incluyendo la mención de dicho país y la documentación de garantías adecuadas; (vi) los periodos previstos para la supresión de las distintas categorías de datos personales; (vii) una descripción general de las medidas de seguridad técnicas y organizativas.

Supervisor de protección de datos o coordinador de protección de datos o **CPD** hace referencia a la persona descrita en el apartado 5.

Datos personales hace referencia a toda la información (incluyendo datos personales de categorías especiales) referidos a la persona en cuestión, por tanto referidos a una persona natural identificada o identificable, como p. ej. nombre, fecha de nacimiento, dirección de correo electrónico, religión, datos en línea (dirección IP, datos de localización, etc.), números de identificación (número de la seguridad social, número de identificación personal, etc.), características físicas (sexo, color de la piel, color de pelo, color de ojos, etc.), datos de cliente, y más) que se rigen por el reglamento de protección de datos aplicable.

Tratamiento o **tratar** hace referencia a todo proceso o serie de procesos automatizados con o sin ayuda relacionados con datos personales, como recopilar, registrar, organizar, clasificar, guardar, adaptar o modificar, leer, consultar, utilizar, revelar mediante transmisión, difusión u otra forma de facilitación, comparar, vincular, limitar, suprimir o destruir.

Seudonimización hace referencia al tratamiento de datos personales de forma que los datos personales ya no se puedan asignar a una persona específica en cuestión sin consultar información adicional, siempre y cuando esta información adicional se conserve por separado y se someta a medidas técnicas y organizativas que garanticen que los datos personales no se pueden asignar a una persona natural identificada o identificable.

Datos personales de categorías especiales hace referencia a datos sobre la raza o el origen étnico, la opinión política, las creencias religiosas o filosóficas, las condenas penales, la pertenencia a un sindicato, la salud o la orientación sexual del interesado o datos genéticos o biométricos con la finalidad de identificar de forma unívoca a una persona natural.

Terceros países son todas las naciones que no son un país de la Unión Europea o del Espacio Económico Europeo o un país con un nivel de protección de datos adecuado que sea considerado adecuado por la Comisión Europea (compárese con la lista de países con un nivel de protección de datos adecuado:

< https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Terceros hace referencia a personas que no sean el interesado, el responsable o el encargado del tratamiento (incluyendo, por ejemplo, socios comerciales, subcontratistas, agencias crediticias y otros), así como personas que están autorizadas a tratar datos personales bajo la autoridad directa del responsable o encargado del tratamiento. En caso de tratamiento de datos personales con permiso, los encargados del tratamiento legalmente no son terceros en el marco de la ley de protección de datos, ya que han sido asignados legítimamente al responsable.

3 ALCANCE

3.1 Alcance organizativo

Esta directriz de protección de datos se aplica a todas las sociedades del consorcio de Arbonia, a todos los empleados de Arbonia y a todos los miembros del Consejo de administración de Arbonia AG. Se debe aplicar de forma jurídicamente vinculante en toda la sociedad del consorcio.

3.2 Leyes, normativas, normas y directrices

Esta directriz de protección de datos incluye todos los requisitos del RGPD y de los principios de protección de datos reconocidos a nivel internacional, sin sustituir a la legislación nacional existente. Complementa a las leyes de protección de datos de aplicación nacional. En caso de conflicto con esta directriz de protección de datos o de que existan requisitos más estrictos que los de esta directriz de protección de datos, tiene prioridad la legislación nacional pertinente. Los contenidos de esta directriz de protección de datos también se deben tener en cuenta cuando no exista legislación nacional pertinente.

Si esta directriz de protección de datos contradice las disposiciones de un determinado país, entonces se pueden adoptar las disposiciones específicas de esta directriz de protección de datos en una directriz local tras consultar con Head Legal & Compliance. No obstante, no se pueden modificar los contenidos básicos y la finalidad de las disposiciones afectadas.

4 BASE REGULADORA

La directriz de protección de datos se basa en el RGPD y en los principios básicos de protección de datos aceptados a nivel mundial.

5 FUNCIONES Y RESPONSABILIDADES

- El director de una sociedad del consorcio[1] es responsable de:
  1. Asegurar en última instancia que la persona jurídica respectiva cumple sus obligaciones legales en cuanto al procesamiento de datos personales.
  2. Asegurar que se cumplen los requisitos de esta directriz de protección de datos (incluyendo la notificación en caso de incidentes en el ámbito de la protección de datos).
  3. Asegurar que el "Directorio de procedimientos de tratamiento" es rellenado y mantenido a nivel de la sociedad del consorcio por el propietario del proceso empresarial.
  4. Nombrar un supervisor de protección de datos local formal (interno o externo) (en lo sucesivo el "supervisor de protección de datos") si se exige en el reglamento de protección de datos local aplicable y esta persona nombrada se debe anunciar anualmente a mediados de año a Head Legal & Compliance e Internal Audit.
  5. Designar a un jefe de protección de datos local (en lo sucesivo, el "coordinador de protección de datos") si el reglamento de protección de datos aplicable a nivel local no prescribe un supervisor de protección de datos local formal. Esta persona nombrada se debe anunciar anualmente a mediados de año a Head Legal & Compliance e Internal Audit.

- El coordinador de protección de datos o supervisor de protección de datos[2] local determinado por el director de una sociedad del consorcio debe:
  1. Monitorizar el cumplimiento de esta directriz de protección de datos y las instrucciones del responsable o el encargado del tratamiento respecto a la protección de los datos personales, incluyendo el traspaso de responsabilidades y las comprobaciones correspondientes.
  2. Informar, asesorar y supervisar al responsable o encargado del tratamiento y a los empleados que realizan obligaciones de tratamiento en el marco de esta directriz de protección de datos.
  3. Dar consejos, a petición, sobre un análisis del impacto de la protección de datos para los datos personales y monitorizar sus resultados, así como responder a otras cuestiones sobre datos personales que se le hayan asignado en el marco de esta directriz de protección de datos.
  4. Monitorizar y mantener actualizado el "Directorio de procedimientos de tratamiento", el cual es llevado por la sociedad del consorcio respectiva y rellenado por el propietario del proceso empresarial, y confirmar anualmente a mediados de año al director y a Head Legal & Compliance que la lista está completa y actualizada.

[1] Para sociedades del consorcio que no están operativas, se debe fijar esta responsabilidad por separado tras consultar con Head Legal & Compliance.
[2] Para sociedades del consorcio que no están operativas, se debe fijar esta responsabilidad por separado tras consultar con Head Legal & Compliance.

5. Servir como persona de contacto de Head Legal & Compliance y mantenerles al corriente acerca de las responsabilidades, riesgos y problemas relacionados con la protección de los datos personales.
6. Apoyar al IT responsable de la aplicación informática en la comprobación y la autorización de nuevas aplicaciones informáticas a nivel de sociedad del consorcio para el tratamiento de datos personales y cada aplicación informática para el tratamiento de datos personales de categorías especiales desde el punto de vista de la protección de datos.
7. Autorizar la transmisión de datos personales a un tercer país desde el punto de vista de la protección de datos (compárese también a continuación el apartado 14).
8. Servir como punto de contacto local para la autoridad de protección de datos para cuestiones relacionadas con el tratamiento de datos y colaborar con la autoridad de protección de datos.
9. Gestionar las consultas de empleados implicados en el tratamiento de datos personales.
10. Responder a consultas de interesados sobre información de los datos personales que Arbonia posee de ellos, o en caso de una consulta sobre varias sociedades del consorcio de Arbonia, realizar la gestión en coordinación con Corporate IT (comp. también a continuación, apartado 7.4)
11. Comprobar y autorizar contratos o acuerdos con el encargado del tratamiento previamente comprobados o elaborados por el propietario del proceso empresarial que pueden ocuparse de los datos personales por encargo de Arbonia como en el apartado 7.2.
12. Monitorizar al supervisor de protección de datos local externo, siempre y cuando se haya nombrado a uno.
13. Notificar las incidencias en el marco de la seguridad de datos según la directriz Data Breach Notification (comp. con el siguiente apartado 9 así como "Arbonia Data Breach Policy").

- El IT-Board, junto con Corporate IT, es responsable de:
  1. Definir estándares válidos a nivel de consorcio, así como IT Controls (GITC), que se deben tener en cuenta para el almacenamiento de datos.

- El IT respectivo que se ocupa de la sociedad del consorcio es responsable de:
  1. Asegurar mediante los correspondientes estándares, políticas y la realización de controles informáticos generales (GITC) que los sistemas, las prestaciones y el equipamiento que se usa para el almacenamiento de datos satisfacen estándares de seguridad aceptables (controles de acceso/supresión de datos) teniendo en cuenta el estado de la técnica, los costes de aplicación y el tipo, el alcance, la conexión y la finalidad del tratamiento, así como las distintas contingencias y la gravedad de las repercusiones en los derechos y las libertades de personas naturales.
  2. Procurar que el responsable y el encargado del tratamiento apliquen medidas técnicas y organizativas adecuadas para asegurar un nivel de protección correspondiente al riesgo, como se especifica en el apartado 8.

3. Tras consultar al coordinador de protección de datos o al supervisor de protección de datos, comprobar y autorizar nuevas aplicaciones informáticas para el tratamiento de datos personales desde el punto de vista de la protección de datos.
4. Realizar comprobaciones y escaneos regulares para garantizar que el hardware y el software de seguridad funcionan correctamente. Los resultados de los controles de protección de datos se deben notificar al supervisor de protección de datos responsable.
5. Evaluar la seguridad de datos de todos los servicios de terceros (p. ej. encargado del tratamiento) que la empresa considera para el tratamiento de datos personales (por ejemplo, servicios de Cloud-Computing, etc.)
6. Llevar una lista de incidencias en el ámbito de la seguridad de datos y notificar las incidencias en el ámbito de la seguridad de datos a Corporate IT.
7. Coordinar y responder a consultas de interesados sobre información de los datos personales que la sociedad del consorcio de Arbonia responsable posee del interesado a través del IT respectivo (comp. también a continuación el apartado 7.4)
8. Notificar las incidencias o riesgos descubiertos en el marco de la seguridad de datos de forma análoga a la directriz Data Breach Notification (comp. con el siguiente apartado 9 así como "Arbonia Data Breach Policy")

- Corporate IT, en colaboración con el IT responsable de la asistencia de una sociedad del consorcio, es responsable de:
  1. Realizar comprobaciones y escaneos regulares para garantizar que el hardware y el software de seguridad funcionan correctamente. Los resultados de los controles de protección de datos se deben notificar al supervisor de protección de datos responsable.
  2. Llevar una lista central de incidencias en el ámbito de la seguridad de datos.
  3. Notificar las incidencias o riesgos descubiertos en el marco de la seguridad de datos de forma análoga a la directriz Data Breach Notification (comp. con el siguiente apartado 9 así como "Arbonia Data Breach Policy").

- Internal Audit es responsable de:
  1. Comprobar, con motivo de las auditorías realizadas según una planificación de auditoría ordenada en el marco de una comprobación basada en riesgos, si los procedimientos obligatorios se corresponden con las especificaciones esenciales de esta directriz de protección de datos.

- El propietario del proceso empresarial es responsable de:
  1. Asegurar que el supervisor de protección de datos local participe de forma adecuada y sin demora en todas las cuestiones necesarias para evaluar el tratamiento de los datos personales.
  2. Comprobar previamente o elaborar todos los contratos o acuerdos con el encargado del tratamiento que pueden ocuparse de los datos personales por encargo de Arbonia como se describe en el apartado 7.2.

3. Rellenar y mantener actualizado el "Directorio de procedimientos de tratamiento", guiado por la sociedad del consorcio respectiva y confirmar anualmente a finales de abril al coordinador de datos o al supervisor de protección de datos que las entradas están completas y actualizadas.
4. Antes de la implementación de nuevos procedimientos de tratamiento de los datos personales, evaluar los riesgos resultantes para la personalidad y los derechos básicos del interesado y, en caso de un riesgo elevado, realizar un análisis del impacto de la protección de datos antes del tratamiento.

6 PRINCIPIOS DE PROTECCIÓN DE DATOS PARA EL TRATAMIENTO DE DATOS PERSONALES

Cada sociedad del consorcio que realiza el tratamiento de datos personales en calidad de responsable debe garantizar que el cumplimiento de los siguientes **6 (seis) principios básicos de protección de datos esenciales se puede demostrar:**

1. Realizar el tratamiento de datos personales solo si se puede demostrar una base jurídica válida en el marco de las leyes de protección de datos aplicables y si se informa al interesado acerca de la identidad y los datos de contacto del responsable, del tipo y las bases jurídicas de los datos personales registrados y de la finalidad para la cual se registran los datos personales

2. Tener en cuenta siempre la finalidad para la que se registran los datos personales

3. Registrar/tratar solo aquellos datos personales que realmente sean necesarios

4. Tratar de forma correcta los datos personales y suprimir los datos personales incorrectos

5. Conservar los datos personales solo durante los periodos de conservación legales realmente necesarios

6. Tratar de forma confidencial los datos personales y compartir solo lo que realmente se deba compartir

6.1 Equidad, legalidad y transparencia

Solo se puede realizar el tratamiento de datos personales para los fines permitidos descritos a continuación; esto se debe realizar de manera transparente. Por tanto, el tratamiento de los datos personales se debe realizar de una forma justa y legítima y se deben tener en cuenta los derechos individuales del interesado. Esto puede incluir datos personales que

Arbonia obtiene directamente del interesado (por ejemplo al rellenar formularios o mediante la correspondencia con nosotros por correo postal, teléfono, correo electrónico u otro), así como datos personales que Arbonia obtiene de terceros.

En el marco de las leyes de protección de datos aplicables se puede realizar el tratamiento de datos personales de forma legítima en base a uno de **cinco principios legítimos** (los **principios legítimos**) según el RGPD. Estos principios incluyen:

1. **Contrato:** El tratamiento de datos personales se requiere para el cumplimiento de un contrato en el cual el interesado es un socio de contrato o para la realización de medidas precontractuales que se realizan a petición del interesado, o

2. **Consentimiento:** El tratamiento de datos personales se basa en el consentimiento (modelo opt-in) del interesado para uno o varios fines específicos. El consentimiento debe estar documentado, o

3. **Obligación legal:** El tratamiento de datos personales se basa en una obligación legal de Arbonia. El tipo y el alcance del tratamiento de los datos debe ser necesario para la actividad de tratamiento permitida legalmente y debe respetar las condiciones legales vigentes, o

4. **Interés público:** El tratamiento se requiere para la salvaguardia de una tarea de interés público o

5. **Intereses comerciales fundados:** El tratamiento es proporcional a los intereses comerciales fundados de Arbonia o terceros a los que se divulgan los datos personales, salvo cuando los intereses o derechos básicos y libertades básicas del interesado prevalezcan sobre estos intereses. Los intereses fundados son, en general, de tipo legal (p. ej. entrada de deudas pendientes/por acuerdo tarifario con el comité de empresa/reivindicación/ejercicio de o defensa contra pretensiones legales relativas al interesado) o comercial (p. ej. evitar incumplimientos de contrato).

La transparencia exige que se deba informar al interesado acerca de cómo se manejan sus datos personales. Por tanto, en general se recomienda registrar los datos personales directamente del interesado (y no a través de terceros). Si se realiza el tratamiento de datos personales se debe informar al interesado acerca de lo siguiente:

- El nombre y los datos de contacto del responsable y, dado el caso, de su representante en la UE
- Dado el caso, los datos de contacto del coordinador de protección de datos o supervisor de protección de datos
- La finalidad del tratamiento de los datos personales, así como la base jurídica para el tratamiento,

- Terceros destinatarios o categorías de terceros destinatarios a los que se pueden transferir datos
- Si procede, información sobre el tratamiento en un tercer país y referencia a garantías adecuadas

6.2 Acotamiento

Solo se puede realizar el tratamiento de los datos personales para la finalidad que se ha comunicado al interesado antes del registro de los datos personales. Las siguientes modificaciones de la finalidad solo son posibles con un alcance limitado y requieren un fundamento. El responsable debe informar al interesado acerca de la finalidad para la que Arbonia realiza el tratamiento de sus datos personales cuando Arbonia los recoge por primera vez o lo antes posible posteriormente. En el caso de todo tratamiento para fines publicitarios o para programas de marketing, se debe conceder al interesado un derecho de oposición contra el tratamiento de sus datos personales y se le debe informar de ello expresamente. En este sentido, todo responsable debe implementar un procesamiento de quejas que garantice que se respetan los procedimientos de opt-out.

6.3 Minimización de datos

Tratar solo aquellos datos personales que realmente sean necesarios. Antes del tratamiento de los datos personales se debe estipular si y con qué alcance es necesario el tratamiento de los datos personales para lograr la finalidad para la cual se realiza. Los datos personales no se pueden registrar con antelación y guardarse para fines futuros potenciales, siempre y cuando esto no se exija o permita en el marco de la legislación nacional.

6.4 Correctos y actuales

Los datos personales deben ser correctos, completos y, si se producen modificaciones, mantenerse actualizados. Se deben dar los pasos adecuados para garantizar que se suprimen, rectifican, complementan o actualizan los datos personales incorrectos o incompletos. Todos aquellos que trabajan con datos personales deben dar los pasos adecuados para ello (por ejemplo, mediante la confirmación de los datos del interesado cuando este hace una consulta o la supresión de un número de teléfono guardado en la base de datos si el interesado ya no lo usa).

6.5 Duración de conservación limitada

Los datos personales solamente se pueden conservar durante la duración de almacenamiento realmente necesaria. Se deben suprimir los datos personales en cuanto ya no se requieran para los fines previstos o se revoque el consentimiento o si se objeta al uso en base a un interés fundado y Arbonia no puede alegar motivos fundados prioritarios. En algunos casos, los periodos de almacenamiento más prolongados pueden permitirnos conservar los datos personales durante más tiempo si se exige legalmente (p. ej. en el marco

del derecho comercial o tributario) o si se requieren datos personales para reivindicaciones, el ejercicio o la defensa de pretensiones legales.

6.6 Confidencialidad y seguridad de datos

Los datos personales se deben tratar siempre de forma confidencial y compartirse solamente como realmente se deben compartir. El principio de "información necesaria" se aplica de modo que los empleados y terceros solamente tienen acceso a los datos personales si y en la medida en que sea necesario para el cumplimiento del fin. Esto requiere un concepto minuciosamente diseñado que defina los derechos de acceso específicos para cada proceso empresarial, incluyendo la aplicación y la aprobación de funciones y responsabilidades (concepto de derecho de acceso). Se debe informar a los destinatarios de datos personales acerca de la confidencialidad de los mismos **y deben estar sujetos a un acuerdo de confidencialidad/acuerdo de no divulgación** (puede ser parte del contrato de trabajo o similar). Excepción: el destinatario está sujeto a un deber de confidencialidad profesional o legal.

Los datos personales se deben asegurar con medidas técnicas y organizativas adecuadas a fin de evitar el acceso ilegítimo, el tratamiento o la divulgación ilegítimos, así como la pérdida, modificación o destrucción accidental (comp. apartado 8).

7 OTRAS OBLIGACIONES EN EL MARCO DEL RGPD U OTROS REGLAMENTOS DE PROTECCIÓN DE DATOS SIMILARES APLICABLES

7.1 Fundamento de la rendición de cuentas

Una sociedad del consorcio de Arbonia que esté sujeta al RGPD (u otro reglamento de protección de datos similar aplicable) debe garantizar que se puede demostrar el cumplimiento de las leyes aplicables en materia de protección de datos (el fundamento de la "rendición de cuentas"). Por tanto, estas sociedades del consorcio deben aplicar y mantener los siguientes puntos en el marco de esta directriz de protección de datos, además de los requisitos generales, siendo el director de la sociedad del consorcio correspondiente el que debe asegurar en última instancia la aplicación y el mantenimiento:

1. Coordinador de protección de datos local o supervisor de protección de datos local: nombramiento de un coordinador de protección de datos o supervisor de protección de datos local especial

2. Gestión del "Directorio de procedimientos de tratamiento": se debe llevar y mantener actualizado un inventario acerca de las actividades de tratamiento de datos personales

3. Comprobación de legitimación: se debe comprobar el tratamiento legítimo de los datos personales en el marco del cumplimiento de los principios legítimos vigentes,

sobre todo en caso de un tratamiento de categorías especiales de datos personales

4. Control del encargado del tratamiento: celebración de un contrato de tratamiento por encargo con el encargado del tratamiento o en calidad de encargado del tratamiento en caso de producción o recepción de datos personales con permiso según el art. 28 del RGPD.

5. En caso de que haya responsables conjuntos del tratamiento, se debe realizar un acuerdo entre los responsables conjuntos del tratamiento según el art. 26 del RGPD.

6. Se debe informar a los empleados de Arbonia acerca de las actividades de tratamiento de datos personales.

7.2 Reglas para el encargado del tratamiento (sobre todo socios de servicios)

El responsable solo trabaja con encargados del tratamiento que ofrecen suficientes garantías de que se toman las medidas técnicas y organizativas adecuadas, de que el tratamiento de datos personales se realiza de conformidad con los requisitos del artículo 28 del RGPD y de que se garantiza la protección de los derechos del interesado.

Para prestaciones divididas dentro de Arbonia existe un acuerdo que permite transferir datos personales, siempre y cuando exista una base legal legítima para la transferencia de dichos datos personales según las leyes de protección de datos aplicables.

7.2.1 Facilitación de datos personales al encargado del tratamiento (saliente)

El tratamiento de datos personales con permiso significa que se encarga a un proveedor de servicios que realice el tratamiento de los datos personales, sin que se transfiera la responsabilidad para el correspondiente proceso comercial (es decir, proveedor de servicios, servicios de outsourcing). En este caso se debe celebrar un contrato de tratamiento por encargo para el tratamiento de los datos personales con proveedores externos con permiso. La respectiva sociedad del consorcio de Arbonia es la responsable y ostenta toda la responsabilidad para la correcta realización del tratamiento de datos personales por parte del encargado del tratamiento.

El respectivo propietario del proceso empresarial debe garantizar que se usa el acuerdo modelo actual para el tratamiento por encargo u otro contrato similar facilitado por el proveedor de servicios para cumplir los requisitos del artículo 28 del RGPD para la contratación de dicho proveedor de servicios. Alternativamente, un proveedor de servicios puede documentar su cumplimiento de los requisitos de protección de datos si cuenta con un certificado UE adecuado y autorizado. Cualquier discrepancia respecto a una de dichas

normas de seguridad debe ser autorizada por el supervisor de protección de datos o el coordinador de protección de datos en colaboración con Corporate IT. Los contratos existentes se deben revisar en el plazo de un año desde la entrada en vigor de esta directriz de protección de datos y deben contener un acuerdo para el tratamiento por encargo por escrito.

7.2.2 Recepción de datos personales como encargado del tratamiento (entrante)

Si los datos personales son transferidos por un tercero a una sociedad del consorcio de Arbonia, se debe garantizar que los datos personales (i) se pueden usar para el fin previsto, (ii) se recopilan en base a motivos legítimos (se recomienda obtener una confirmación por escrito) y (iii) existe un contrato de tratamiento por encargo que se corresponde con el artículo 28 del RGPD.

7.3 Transferencia transfronteriza de datos personales

En caso de una transferencia transfronteriza de datos personales, se deben cumplir los requisitos nacionales respectivos para la divulgación de datos personales en el extranjero. En el marco del RGPD se puede realizar la transferencia de datos personales dentro de la UE, el EEE o un país que cumpla garantías adecuadas según la Comisión Europea a fin de garantizar un nivel de protección de datos adecuado. Dicha transferencia de datos no requiere un permiso especial. La Comisión Europea ha clasificado a Suiza, entre otros países, como garante de una protección adecuada (comp. la lista de países actual: < https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Solo se permite la transferencia de datos personales a un tercer país si existen garantías adecuadas. Esto significa si el destinatario puede demostrar que mantiene un estándar de protección de datos correspondiente al de esta directriz de protección de datos (p. ej. i) existen reglas empresariales vinculantes, ii) se han firmado cláusulas de contrato estándar de la UE para el tratamiento por encargo en terceros países con el proveedor de servicios y otros subcontratistas[3], iii) existen normas de comportamiento aprobadas por la autoridad de protección de datos, iv) en caso de participación de un proveedor de servicios en un sistema certificado que ha sido acreditado por la UE para alcanzar un nivel de protección de datos suficiente o v) con acuerdos individuales entre el responsable y el encargado del tratamiento con permiso de la autoridad de protección de datos responsable) e informando al interesado. Esta obligación no se aplica si la transferencia se basa en una obligación legal. Dicha transferencia requiere la autorización por parte del coordinador de protección de datos o del supervisor de protección de datos.

[3] Comp. Decisión de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, < https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32010D0087 >

Si se transfieren datos personales dentro de Arbonia, la sociedad del consorcio que importa los datos personales está obligada a cooperar con todas las consultas que realiza la autoridad de protección de datos en el país en el que tiene su sede registrada la sociedad del consorcio exportadora y a cumplir todas las observaciones que hace la autoridad de protección de datos correspondiente respecto al tratamiento de los datos personales transferidos.

7.4 Gestión de las consultas de información por parte de un interesado

Los interesados tienen derecho a realizar una solicitud formal de información acerca de los detalles de los datos personales que Arbonia posee y pueden exigir lo siguiente:

Derecho a la información acerca de:

- los fines del tratamiento;
- las categorías de datos personales que se pueden tratar;
- los destinatarios o categorías de destinatarios a los que se han divulgado o se pueden divulgar los datos personales, en particular en caso de destinatarios en terceros países o en caso de organizaciones internacionales;
- si es posible, la duración planeada durante la cual se pueden guardar los datos personales, o si esto no es posible, los criterios para determinar dicha duración;
- la existencia de un derecho de rectificación o supresión de los datos personales que le afectan o la limitación del tratamiento por parte del responsable o de un derecho de oposición contra dicho tratamiento;
- la existencia de un derecho de apelación a una autoridad de protección de datos;
- toda la información disponible acerca del origen de los datos si los datos personales no se han recopilado a partir del interesado;
- la existencia de una toma de decisiones automatizada, incluyendo profiling;
- Si los datos personales se transfieren a un tercer país o a una organización internacional, el interesado tiene derecho a ser informado de las garantías adecuadas.

Derecho de rectificación:

- El interesado tiene derecho a exigir al responsable la rectificación sin demora de los datos personales incorrectos relativos a él. Teniendo en cuenta los fines del tratamiento, el interesado tiene derecho a exigir que se completen los datos personales incompletos, también mediante una aclaración complementaria.

Derecho de supresión ("derecho al olvido"):

- El interesado tiene derecho a exigir al responsable la supresión sin demora de sus datos personales y el responsable está obligado a suprimir sin demora los datos personales siempre y cuando se aplique uno de los siguientes principios:
    1. Los datos personales ya no se necesitan para los fines para los que se habían recopilado o tratado de otro modo;

2. El interesado revoca su consentimiento, sobre el que se apoya el tratamiento según el artículo 6, apartado 1 letra a del RGPD o el artículo 9 apartado 2 letra a del RGPD y se carece de otra base jurídica para el tratamiento;
3. El interesado formula su oposición al tratamiento según el artículo 21 apartado 1 del RGPD y no existen motivos fundados prioritarios para el tratamiento o el interesado formula su oposición al tratamiento según el art. 21 apartado 2 del RGPD;
4. Los datos personales se han tratado de forma ilegítima;
5. La supresión de los datos personales se requiere para el cumplimiento de una obligación legal según la legislación del Estado Miembro respectivo al que está sujeto el responsable;
6. Los datos personales se han recopilado en relación con servicios ofrecidos de la sociedad de información según el artículo 8 apartado 1 del RGPD.

Derecho a la limitación del tratamiento:

- El interesado tiene derecho a exigir al responsable la limitación del tratamiento si se da uno de los siguientes requisitos previos:
- si el interesado disputa la corrección de los datos personales y durante el tiempo que permita al responsable comprobar la corrección de los datos personales:
- si el tratamiento es ilegítimo y el interesado rechaza la supresión de los datos personales y, en vez de ello, exige la limitación de la utilización de los datos personales;
- si el responsable ya no necesita los datos personales para los fines del tratamiento, pero el interesado los necesita para la reivindicación, el ejercicio o la defensa de pretensiones legales,
- si el interesado ha formulado su oposición al tratamiento según el artículo 21 apartado 1, siempre y cuando todavía no se haya determinado si los motivos fundados del responsable tienen prioridad sobre los del interesado.

Se debe pedir al interesado que ponga por escrito su petición, o bien por correo electrónico o por correo postal, y dirigida al respectivo supervisor de protección de datos local. El supervisor de protección de datos local debe facilitar información al interesado sin demora, pero siempre en el plazo de un mes desde la recepción de la consulta. Este plazo se puede prolongar dos meses si esto fuera necesario en virtud de la complejidad y del número de solicitudes. El coordinador de protección de datos o el supervisor de protección de datos del responsable informa al interesado en el plazo de un mes desde la recepción de su solicitud acerca de la ampliación del plazo, así como de los motivos de la misma. El interesado no puede acarrear con los costes por informarle de la información que posee acerca de él una sociedad del consorcio de Arbonia, siempre y cuando las solicitudes de un interesado no sean claramente excesivas o infundadas, en especial debido a una formulación repetida. Las solicitudes de un interesado a varias sociedades del consorcio de Arbonia se deben remitir a Corporate IT para su coordinación y respuesta.

7.5 Realización de un análisis del impacto de la protección de datos

Si una nueva forma planificada de tratamiento de datos personales tiene previsiblemente como consecuencia un mayor riesgo para los derechos y libertades del interesado en base al tipo, el alcance, las circunstancias y los fines del tratamiento, sobre todo en el caso de la utilización de nuevas tecnologías, se debe realizar previamente un análisis de las consecuencias de los procesos de tratamiento previstos para la protección de los datos personales.

Por tanto, antes de la implementación de nuevos procesos de tratamiento, se deben analizar los riesgos resultantes para la personalidad y los derechos básicos del interesado. En el caso de nuevas aplicaciones informáticas, esto se debe considerar en el marco del proceso de autorización. Si debido a un primer análisis se deduce que la nueva forma planeada de tratamiento de los datos personales tiene previsiblemente como consecuencia un elevado riesgo para el interesado, se debe realizar un análisis del impacto de la protección de datos.

Las consultas sobre la necesidad del análisis del impacto de la protección de datos o durante la realización del mismo, se deben dirigir al coordinador de protección de datos local o al supervisor de protección de datos local. Tras su realización, se debe informar al coordinador de protección de datos local o al supervisor de protección de datos local acerca del análisis del impacto de la protección de datos y se le debe pedir opinión.

Si de un análisis del impacto de la protección de datos se deriva que el tratamiento tendría un elevado riesgo para el interesado y no se toman medidas para mitigar el riesgo, se debe consultar a la autoridad de protección de datos antes de la implementación de los nuevos procedimientos de tratamiento.

8 SEGURIDAD DE LOS DATOS PERSONALES

Los datos personales se deben proteger contra el acceso ilegítimo y contra el tratamiento o divulgación ilegítimos, así como contra la pérdida, modificación o destrucción accidental. Esto se aplica independientemente de si el tratamiento de los datos personales se realiza en papel o de forma electrónica.

El responsable y el encargado del tratamiento deben implementar medidas técnicas y organizativas adecuadas para proteger los datos frente al tratamiento ilegítimo. Estas medidas se deben basar en (i) los mejores procedimientos, (ii) los riesgos del tratamiento y (iii) la necesidad de proteger los datos personales (determinada mediante el proceso para la clasificación de información); incluyen, entre otros, de la forma adecuada:

(a) la seudonimización y el cifrado de datos personales;

(b) asegurar la capacidad, la confidencialidad, la integridad, la disponibilidad y la capacidad de carga de los sistemas y servicios en conexión con el tratamiento a lo largo del tiempo;

(c) restablecer rápidamente la capacidad, la disponibilidad de los datos personales y el acceso a ellos en caso de incidencia técnica o física;

(d) un procedimiento para la comprobación, análisis y evaluación regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad.

Las medidas técnicas y organizativas para la protección de los datos personales son parte de la gestión interna de seguridad de la información y deben adaptarse constantemente a los desarrollos técnicos y las modificaciones organizativas.

Los procedimientos de seguridad deben incluir al menos:

- Controles de acceso: se debe notificar cualquier persona ajena hallada en las áreas con control de acceso.

- Archivadores o cajones que se puedan cerrar de forma segura: el escritorio y los armarios deben permanecer cerrados si contienen información confidencial de cualquier tipo. Los datos personales siempre son información confidencial. Los empleados deben asegurar que los papeles e impresos con datos personales no se dejen visible de forma general, como en una impresora. Si se almacenan datos personales con autorización en un soporte de intercambio de datos (como un CD, una memoria USB o un DVD), este se debe guardar bajo llave cuando no se esté usando.
- Métodos de eliminación: los documentos en papel se deben triturar y desechar de forma segura cuando ya no se necesiten. Esto también se aplica a los datos personales que se guardan habitualmente de forma electrónica, pero se hayan impreso.

- Datos guardados de forma electrónica: los datos personales deben estar protegidos adecuadamente mediante contraseñas de la actual directiva de contraseñas y nunca se deben compartir con los empleados. Si se aplica la forma electrónica, los datos personales se deben guardar y consultar en sistemas de servidores informáticos y en aplicaciones informáticas estructuradas, en vez de sin cifrar en ordenadores locales.

- Datos personales recopilados de forma electrónica que han sido facilitados por el interesado: se debe comprobar la identidad del interesado, preferentemente mediante un proceso doble de opt-in (también mediante un segundo correo electrónico para la validación de la dirección de correo electrónico indicada). Si se limita el acceso a un sitio web o aplicación a los usuarios registrados (es decir, cuenta de usuario), la identificación y autentificación de la persona afectada debe

ofrecer una protección de seguridad que sea proporcional a los contenidos respectivos durante el acceso.

- Precaución al compartir datos personales: nunca se deben compartir de manera informal los datos personales. Se aplica el principio de "información necesaria". Es obligatorio un concepto de desglose y división por proceso empresarial, así como la aplicación de funciones y responsabilidades. Los datos personales se deben cifrar antes de la transferencia en forma electrónica. El jefe de informática puede explicar cómo se envían datos personales a personas de contacto externas autorizadas.

- Pedir instrucciones: en caso de preguntas o incertidumbre acerca de algún aspecto de la protección de datos o de los deberes aplicables de esta directriz de protección de datos, se debe pedir consejo al superior directo, al respectivo supervisor de protección de datos local o a Legal & Compliance.

El RGPD exige tener en cuenta la esfera privada lo antes posible. La esfera privada mediante el diseño de la técnica exige que las organizaciones tengan en cuenta la esfera privada en los primeros niveles del diseño de la técnica y durante todo el proceso de desarrollo de nuevos productos, procedimientos o servicios relacionados con los datos personales. Esfera privada mediante preajuste significa que si un sistema o un servicio incluye la decisión del mismo acerca de cuántos datos personales puede compartir con otro, los ajustes previos deben ser aquellos que ofrezcan la máxima protección para la esfera privada. Por tanto, toda nueva aplicación informática está sujeta a un proceso de aprobación interna en el que se debe evaluar dicha nueva aplicación informática en el marco de la evaluación también desde el punto de vista de la protección de datos.

9 NOTIFICACIÓN DE INCIDENCIAS EN EL ÁMBITO DE LA SEGURIDAD DE DATOS

Muchos reglamentos de protección de datos aplicables exigen una notificación directa de incidencias en el ámbito de la protección de datos a la autoridad legislativa. Por tanto, se exige que todas las incidencias en el ámbito de la seguridad de datos se notifiquen sin demora al coordinador de protección de datos o supervisor de protección de datos responsable, independientemente de si está implicado un sistema local o un sistema del consorcio de conformidad con el proceso descrito en la directriz de Arbonia para incidencias en el ámbito de la seguridad de datos ("Arbonia Data Breach Policy"). Si el IT detecta incidencias o riesgos en el ámbito de la seguridad de datos, se deben notificar de manera análoga a la directriz Data Breach Notification.

El objetivo de este cumplimiento de las obligaciones mediante la notificación de una vulneración de las obligaciones de protección de datos vigentes en el marco de las leyes de protección de datos aplicables (p. ej. en el marco del RGPD, como muy tarde en el plazo de 72 horas desde que se tiene conocimiento de ello).

En dicho caso, se debe hacer énfasis en respetar los plazos respectivos para la notificación de vulneraciones de la protección de datos y tomar medidas sin demora para investigar las incidencias y determinar si realmente se han vulnerado los datos personales. Corporate IT debe llevar un directorio interno de vulneraciones de seguridad en Arbonia, de modo que se puedan cumplir los deberes de notificación en el marco de la legislación nacional y se pueda asegurar que se aplican las normas de representación respectivas para poder notificar las vulneraciones en cualquier momento. Antes de la notificación a una autoridad nacional se debe informar a Corporate IT o al departamento Legal and Compliance del consorcio.

Se deben respetar de forma estricta todas las demás directrices de Corporate IT, así como de los departamentos informáticos locales.

10 CONSECUENCIAS EN CASO DE INCUMPLIMIENTO

El cumplimiento de esta directriz de protección de datos es de suma importancia para Arbonia y para la imagen pública de Arbonia. En muchos países, un tratamiento indebido de los datos personales u otras vulneraciones de las leyes de protección de datos pueden estar sujetos también a sanciones penales y dar lugar a reivindicaciones de indemnización de daños y perjuicios. Dentro de Arbonia, una vulneración de las normas de esta directriz de protección de datos puede acarrear sanciones en el marco de ley y/o del respectivo contrato (de trabajo).

11 DISCREPANCIAS

Solo se permiten discrepancias de las disposiciones de esta directriz y sus añadidos tras consultar con el Head of Legal & Compliance.

12 INFORMACIÓN

El Head of Legal & Compliance proporciona información relacionada con la directriz de protección de datos.

ARBONIA

13 ENTRADA EN VIGOR

Esta directriz entra en vigor el 17 de junio de 2020 y sustituye la directriz acerca del tratamiento de los datos (directriz de protección de datos) del 5 de diciembre de 2013.

Arbon, 16 de junio de 2020

Arbonia AG

Alexander von Witzleben
Presidente del Consejo de administración y CEO

Andrea Wickart
Head of Legal & Compliance/Secretaria general

Añadidos a esta directriz de protección de datos de Arbonia:

Los siguientes añadidos a su versión actual concretan esta directriz de protección de datos:

- Directriz para solicitudes de interesados y para la eliminación de datos
- Directriz para vulneraciones de la protección de datos
- Declaración de protección de datos para empleados

Este documento es válido sin firma.