

# **Reglamento general sobre procesamiento de datos personales en Aplatform, z.ú.**

## **RESUMEN**

El propósito del presente Reglamento consiste en definir las reglas de marco para la gestión de datos personales y documentos que contienen dichos datos personales. También forman parte de las mismas las instrucciones generales sobre la manera de actuar en consonancia con las medidas organizativo-tecnológicas y otras orientadas al cumplimiento de las disposiciones legales vigentes y eficaces para la protección de datos personales, aplicadas en el instituto Aplatform, z.ú., con sede en Bílkova 855/19, Staré Město, 110 00 Praga 1, República Checa, N.I.: 17278457 (en adelante "Aplatform").

Entre otras cosas de manera general el Reglamento estipula el propósito y el alcance de la recopilación y procesamiento de datos personales, los medios y formas de su tratamiento, así como los derechos y obligaciones de las personas relacionadas con dichos datos y la gestión de los mismos. Proteger los datos personales es la obligación tanto del instituto Aplatform, como de cada uno de sus trabajadores, empleados y de cualquier otra persona que desempeñe tareas para Aplatform ("trabajadores"). Las reglas concretas relacionadas con los subtipos de procesamiento de datos personales (por ejemplo el procesamiento de datos ocupacionales, datos de usuarios de la aplicación Sangha, páginas web [www.mahasangha.net](http://www.mahasangha.net), datos de suministradores, etc.) están comprendidas en las sub-reglas internas del instituto Aplatform, a las que se remite el Reglamento.

## **PRINCIPIOS BÁSICOS**

Al gestionar los datos personales Aplatform y todos sus trabajadores tienen la obligación de observar el GDPR y la ley sobre procesamiento de datos personales. Ante todo el GDPR estipula las reglas y principios que rigen en el tratamiento de datos personales y Aplatform asume dichos principios.

## **PRINCIPIOS DE PROCESAMIENTO DE DATOS PERSONALES**

### **1. Legalidad, correctitud y transparencia:**

Todos los datos personales procesados en el instituto Aplatform en relación con el sujeto de datos deben ser tratados de manera correcta, legal y transparente;

### **2. Restricciones especiales:**

Es posible recopilar datos personales únicamente para ciertos propósitos, expresamente manifestos y legítimos y éstos no deben ser procesados posteriormente de manera incompatible con estos propósitos;

### **3. Minimización de datos:**

Se permite procesar datos personales únicamente en el alcance indispensable para cumplir el propósito estipulado;

### **4. Precisión:**

Solo se pueden procesar los datos personales precisos y en caso de necesidad los datos personales actualizados; deben adoptarse todas las medidas sensatas para que los datos personales inexactos,

teniendo en cuenta los propósitos de su procesamiento, sean inmediatamente cancelados o corregidos;

#### **5.Limitaciones de almacenamiento:**

Los datos personales se pueden almacenar de manera que faciliten la identificación de los sujetos de datos únicamente por un tiempo no más largo que el indispensable para los propósitos de su tratamiento;

#### **6.Integridad y confidencialidad:**

Los datos personales pueden ser procesados únicamente asegurando la protección adecuada de los mismos mediante medidas tecnológicas u organizativas, contra el procesamiento ilegítimo o ilegal, la pérdida casual, destrucción o deterioro;

#### **7.Responsabilidad:**

El instituto Aplatform debe ser capaz de demostrar que cumple los principios mencionados, incluida la conformidad con las disposiciones legales vigentes y eficaces para la protección de datos personales;

#### **8.Enfoque basado en el grado de riesgo (el llamado Risk Based Approach):**

Cuanto más alto es el riesgo de que el tipo de procesamiento realizado por el instituto Aplatform pueda intervenir en los intereses o derechos básicos y libertades del sujeto de datos, es preciso adoptar medidas de lo más estrictas conducentes a la transparencia y seguridad del procesamiento existente. Si el trabajador concreto que gestiona los datos personales no está seguro del riesgo vinculado con el tratamiento, o de las obligaciones concretas que le atañen en relación con el procesamiento de datos personales, se dirigirá a la persona responsable del procesamiento de datos personales en Aplatform.

### **REGLAS CONCRETAS**

#### **1. COMPETENCIA**

- 1.1. El Reglamento es una disposición interna normativa que compromete a todos los empleados y demás trabajadores, así como a las personas que colaboran con el instituto Avato y también a otras personas sujetas a las reglas internas del instituto Aplatform, así como a las personas que se hayan comprometido a cumplir el presente Reglamento en el marco de su relación con el instituto Aplatform o con el procesador.
- 1.2. El instituto Aplatform tiene la obligación de asegurar que las personas que tratan los datos personales, sobre la base de un acuerdo con el instituto Aplatform, se comprometan a cumplir las disposiciones del presente Reglamento.
- 1.3. Aplatform designará a la persona que supervisará el cumplimiento del presente Reglamento dentro del marco de la organización interna.

#### **2. DEFINICIONES BÁSICAS**

##### **Las personas que gestionan datos personales y el sujeto de los datos**

**(a) Administrador:** Sujeto que por si mismo o junto con otros determina los propósitos y los medios para el procesamiento de datos personales o que tiene la obligación de procesar datos personales de conformidad con las disposiciones legales vigentes y eficaces; se considera que **Aplatform** es el administrador para los fines del presente Reglamento;

**(b) Procesador:** Persona (física o jurídica) que procesa los datos personales para el administrador;

**(c) Sujeto de los datos:** Persona física identificada o no identificada (de ningún modo persona jurídica: sociedad u organización).

### **Datos personales y tipos de los mismos**

**(d) Datos personales:** Todas las informaciones sobre una persona física (sujeto de datos) que se pueda identificar directa o indirectamente, sobre todo con referencia a un identificador concreto, por ejemplo nombre, fecha de nacimiento, número de identificación, datos de dirección o de contacto, datos de localización o identificador de red. Se consideran datos personales también aquellos que de por sí no se refieren a una persona física, aunque en unión con otras informaciones podrían vincularse (solo potencialmente) con una persona física concreta;

**(e) Categorías especiales de datos personales:** Un dato personal que testimonia del origen racial o étnico, de opiniones políticas, religión o convencimiento filosófico, o militancia en sindicatos y tratamiento de datos genéticos, datos biométricos con el fin de identificar exclusivamente a la persona física, y datos sobre el estado de salud o vida sexual u orientación sexual de la persona física; los datos relativos a condenas por delitos penales se benefician de especial protección;

**(f) Datos biométricos:** Datos personales que se desprenden de signos físicos o fisiológicos de la persona, por ejemplo la representación de la cara, los datos sobre huellas dactilográficas, etc.;

**(g) Dato anónimo:** Un dato que en su forma original o una vez procesado no puede ser atribuido a un determinado o un determinable sujeto de datos: de hecho no se trata de un dato personal.

### **Procesamiento de datos personales**

**(h) Procesamiento de datos personales:** Cualquier operación con datos personales, como por ejemplo recopilación, anotación, ordenación, estructuración, almacenamiento, adaptación o modificación, selección, consulta, uso, ordenamiento, accesibilidad, aunque también cancelación o destrucción;

**(i) Recopilación de datos personales:** Procedimiento sistemático, cuyo objetivo consiste en obtener datos personales con el propósito de su siguiente almacenamiento en un soporte de datos para su inmediato o posterior procesamiento;

**(j) Almacenamiento de datos personales:** Mantenimiento de datos en tal forma que facilite su posterior procesamiento;

**(k) Eliminación de datos personales:** Destrucción física del soporte, cancelación física o exclusión permanente de posteriores procesamientos; en forma de eliminación de datos personales es **anonimización**;

**(l) Anonimización:** Actividad durante la que se produce la cancelación permanente o el desacoplamiento de los identificadores, con la ayuda de los que sería posible identificar a una persona física concreta;

**(m) Seudonimización:** Procesamiento de datos personales de forma que ya no puedan ser asignados a un sujeto concreto sin emplear informaciones suplementarias, siempre que estas informaciones suplementarias sean almacenadas separadamente; después de reincorporar las informaciones suplementarias que sea posible volver a identificar la persona física concreta;

**(n) Perfilaje:** Tratamiento automatizado que consiste en usar los datos personales para evaluar, analizar o apreciar algunos aspectos personales de la persona física, relativos por ejemplo a su

rendimiento laboral, situación económica, preferencias personales, intereses, comportamiento, lugar en el que se encuentra, etc.

### **Siguientes**

**(o) Violación del aseguramiento de los datos personales:** Violación del aseguramiento que lleva a la destrucción, pérdida, alteración o entrega ilegítima o acceso casual o ilegal de datos personales transmitidos o almacenados o procesados de forma distinta;

**(p)** El término **Reglamento** significa el presente Reglamento general sobre procesamiento de datos personales;

**(q) GDPR:** Reglamento del Parlamento Europeo y del Consejo (UE) 2016/679 sobre la protección de personas físicas en relación con el tratamiento de datos personales y sobre la libre circulación de dichos datos y cancelación de la Directiva 95/46/CE (Reglamento general sobre protección de datos personales);

**(r) Ley sobre el tratamiento de datos personales:** ley no. 110/2019 Col., sobre tratamiento de datos personales.

## **3. PROPÓSITO Y ALCANCE DEL TRATAMIENTO DE DATOS PERSONALES**

- 3.1. Las personas obligadas por el presente Reglamento tienen el derecho a recopilar y procesar datos personales o entregar dichos datos a otras personas únicamente para el propósito y de forma estipulada en las disposiciones internas de Aplatform o según la instrucción o la especificación de la persona responsable del procesamiento de datos personales en Aplatform.
- 3.2. Los datos personales pueden ser entregados únicamente a otras personas mencionadas en las disposiciones internas de Aplatform, o bien si la entrega de los mismos a estas personas ha sido autorizada por la persona responsable del procesamiento de datos personales en Aplatform (exceptuando la entrega o el acceso de las respectivas autoridades estatales y otras personas, de conformidad con disposiciones legales especiales, por ejemplo la Policía de la RCh). Lo mismo se aplica para la entrega de datos personales al extranjero.
- 3.3. Las personas obligadas por el presente Reglamento se rigen por el esquema de retención en vigor y no almacenan datos personales en contradicción con el principio de limitación del almacenamiento o con el presente Reglamento. Una vez expirado el tiempo estipulado en el esquema de retención o después de haber desaparecido el propósito para el que los datos personales fueron almacenados, es preciso destruir los datos personales de acuerdo con las disposiciones internas de Aplatform o con las instrucciones de la persona responsable del procesamiento de datos personales Aplatform.

*Extracto del esquema de retención en vigor para la aplicación Sangha*

## **4. MEDIOS Y FORMA DE PROCESAMIENTO DE DATOS PERSONALES**

- 4.1. Al procesar datos personales es preciso elegir los medios apropiados desde el punto de vista del propósito del procesamiento. Es preciso proceder de manera a que el sujeto de datos no sufra mengua en sus derechos, sobre todo el derecho a preservar su dignidad humana; y también es necesario acatarse a la protección ante la injerencia ilegal en la vida privada y personal del sujeto de datos.

<b>Aplatform, z.ú.</b>					
Esquema de retención para la aplicación Sangha					
<i>Categoría</i>	<i>Descripción</i>	<i>Plazo mínimo estipulado para su almacenamiento</i>	<i>Referencia</i>	<i>Plazo prolongado para su almacenamiento (uso)</i>	<i>Nota</i>
<b>Base de datos de los usuarios de la aplicación móvil Sangha</b>	Base de datos de los usuarios de la aplicación móvil Sangha	Se guarda durante el plazo de su registración	Condiciones para el uso de la aplicación Sangha		-
	Base de datos de los usuarios de la aplicación móvil Sangha, a los que se canceló la cuenta debido a la violación de las Condiciones de uso	Se guarda durante el plazo de 10 años desde la cancelación de la cuenta de usuario	Condiciones de uso de la aplicación móvil Sangha		-

- 4.2. La disposición interna de Aplatform estipula si es posible tratar los datos personales de los sujetos de datos sin el consentimiento de dichos sujetos de datos, o únicamente sobre la base de su consentimiento.
- 4.3. En los casos en que es posible tratar los datos personales únicamente sobre la base del consentimiento de los sujetos de datos, las disposiciones internas de Aplatform o la persona responsable del tratamiento de datos personales en Aplatform establecerá el texto que se entregará a los sujetos de datos antes de haberse conseguido los datos personales o antes de otro inicio del tratamiento de los mismos.
- 4.4. En los casos en que es posible tratar los datos personales aun sin el consentimiento de los sujetos de datos, la disposición interna de Aplatform o la persona responsable del tratamiento de datos personales en Aplatform establecerá qué informaciones e instrucciones deben ser entregadas a los sujetos de datos (sea en forma de documento escrito, u oralmente: por ejemplo en caso de contacto telefónico con el sujeto de datos) antes de haber obtenido los datos personales o antes de otro inicio del tratamiento de los mismos.
- 4.5. Las personas obligadas por el presente Reglamento tienen el derecho de procesar datos personales solo en la forma estipulada en las disposiciones internas de Aplatform o según las instrucciones de la persona responsable del procesamiento de datos personales en Aplatform. Los documentos físicos que contienen datos personales pueden ser almacenados y procesados solo dentro del marco de espacio del instituto Aplatform, a saber en los lugares previamente destinados al almacenamiento o manipulación de los mismos. Los documentos electrónicos pueden ser procesados únicamente mediante sistemas previamente designados, mientras que la manipulación de datos personales dentro del marco de los sistemas está registrada por Aplatform, lo que facilita designar y comprobar cuándo, quién y por qué razón los datos personales fueron anotados o procesados de forma distinta.
- 4.6. Todos los datos personales o documentos que contienen datos personales deben ser procesados en consonancia con los principios de protección mencionados en las disposiciones internas especiales del instituto Aplatform.

## **5. DERECHOS DE LOS SUJETOS DE DATOS**

- 5.1. Según el GDPR los sujetos de datos tienen la posibilidad de aplicar su derecho a exigir del instituto Aplatform:

- (i) acceso a sus datos personales;
- (ii) enmienda de datos personales;
- (iii) cancelación de datos personales;
- (iv) limitación del procesamiento de datos referentes al sujeto de datos;
- (v) derecho a objetar contra el procesamiento; y
- (vi) derecho a la portabilidad de datos.

5.2. En caso de que cualquier persona obligada por el presente Reglamento reciba una solicitud relacionada con la aplicación del derecho de los sujetos de datos según el artículo 5.1 (i), procederá de acuerdo con el artículo 6; en los demás casos trasladará la solicitud a la persona responsable del procesamiento de datos personales en Aplatform.

## **6. OBLIGACIÓN DE INSTRUIR E INFORMAR, DERECHO DE ACCEDER A LOS DATOS**

- 6.1. En caso de que el instituto Aplatform haya conseguido los datos personales del sujeto de datos tiene la obligación de instruirlo al tenor del artículo 13 del GDPR. Para este propósito asegurará que el sujeto de datos se familiarice debidamente con el texto instructivo y que confirme este hecho con su firma o con otra manifestación de voluntad demostrable.
- 6.2. En caso de que los datos personales no hayan sido adquiridos del sujeto de datos, el instituto Aplatform tiene la obligación de instruirlo al tenor del artículo 14 del GDPR. Para este propósito asegurará que el sujeto de datos se familiarice debidamente con el texto instructivo y que confirme este hecho con su firma o con otra manifestación de voluntad demostrable.
- 6.3. Las informaciones mencionadas en el artículo 6.1 las entregará Aplatform al sujeto de datos en el momento en que adquiera los datos personales y las informaciones mencionadas en el artículo 6.2. Aplatform las entregará al sujeto de datos en un plazo apropiado tras haber recibido los datos personales pero a más tardar a los 30 días. En los casos en que los datos personales deben ser usados para fines de comunicación Aplatform entregará dichas informaciones en el momento en que se produzca por primera vez esa comunicación, o bien si los datos personales deben ser accesibles para otro beneficiario, Aplatform brindará la información en el momento en que los datos personales sean accesibles.
- 6.4. Si el sujeto de datos aplica su derecho a acceder a sus datos personales según el artículo 15 del GDPR, el instituto Aplatform tiene la obligación de entregarle la información, sin dilación, a más tardar a los 30 días después de haber recibido la solicitud. Las informaciones se brindan en la forma en la que el sujeto de datos aplica su derecho.
- 6.5. Antes de comunicar la información sobre el procesamiento dentro del marco del derecho aplicado al acceso por parte del sujeto de datos, el instituto Aplatform tiene la obligación de verificar la identidad del sujeto de datos que plantea la pregunta. Para verificar la identidad del sujeto de datos que solicita acceso a datos personales, Aplatform aplicará todas las medidas adecuadas. Si el instituto Aplatform no es capaz de identificar suficientemente al sujeto de datos, le informará de este extremo, siempre que sea posible. No se abusará de la verificación de la identidad para adquirir otros datos o para su almacenamiento con otros propósitos que no sea la reacción a la solicitud concreta del sujeto de datos.
- 6.6. El contenido de la información mencionada en el artículo 6.4 informa sobre:
  - (a) el propósito del procesamiento de datos personales,
  - (b) los datos personales, eventualmente sobre las categorías de datos personales que son objeto del procesamiento,

- (c) el beneficiario, eventualmente las categorías de beneficiarios,
- (d) el plazo durante el que los datos personales serán almacenados,
- (e) la existencia del derecho a exigir que el instituto Aplatform corrija o cancele los datos personales relativos al sujeto de datos o limite su procesamiento o presente una objeción contra dicho procesamiento,
- (f) el derecho a presentar una queja ante la Oficina de protección de datos personales,
- (g) todas las informaciones accesibles y la fuente de datos personales, siempre que no sean adquiridas del sujeto de datos, y
- (h) el hecho de que suelen tomarse decisiones automatizadas, incluido el perfilaje y en esos casos informaciones sensatas relativas al procedimiento aplicado, así como informaciones sobre la importancia de las supuestas consecuencias de dicho procesamiento para el sujeto de datos.

6.7. La información según el artículo 6.6 se entrega en forma electrónica, corrientemente usada, siempre que el sujeto de datos no solicite que se proceda de manera distinta.

## **7. PARTICIPACIÓN DEL ANALISTA DE DATOS PERSONALES**

- 7.1. El instituto Aplatform puede encargar el procesamiento de datos personales a una tercera persona (analista), que ofrece suficientes garantías para introducir medidas tecnológicas y organizativas adecuadas con el fin de asegurar la protección de los derechos de los sujetos de datos.
- 7.2. El encargo, según el apartado anterior, puede ser concedido solo dentro del marco del contrato sobre procesamiento de datos personales que debe estar en forma escrita.

## **8. PERSONAS COMPETENTES Y ALCANCE DE SU COMPETENCIA**

- 8.1. Los trabajadores concretos de Aplatform tienen roles adjudicados en el marco de los que pueden acceder y tratar datos personales concretos para propósitos concretos.
- 8.2. Nadie puede tratar datos personales más allá del marco de su competencia, como se especifica en la descripción de cada uno de los roles y la incorporación de los trabajadores concretos en cada uno de dichos roles.
- 8.3. La persona competente por el tratamiento de datos personales en Aplatform puede expresamente conceder excepciones individuales a las reglas mencionadas más arriba.

## **9. OBLIGACIÓN DE CONFIDENCIALIDAD**

- 9.1. Todas las personas que procesen datos personales para Aplatform, así como otras personas que entren en contacto con datos personales en Aplatform o con el analista, tienen la obligación de mantener la confidencialidad respecto de los datos personales y de las medidas de seguridad adoptadas según el presente Reglamento u otras disposiciones del instituto Aplatform. La obligación de confidencialidad persiste incluso una vez terminados los respectivos trabajos.

## **10. VIOLACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES**

- 10.1. Cualquier caso de violación de la protección de datos personales, sobre todo la pérdida, el hurto, el deterioro o la destrucción de los mismos (al margen del riesgo de injerencia en los derechos de los sujetos de datos relacionados con un caso concreto de violación de la protección de datos personales) de los que toda persona se entere, tendrá la obligación de comunicarlo, sin dilación, a su superior y al mismo tiempo a la persona responsable del procesamiento de datos personales en Aplatform.
- 10.2. Las personas obligadas por el presente Reglamento tienen la obligación de comunicar, al tenor del epígrafe anterior, incluso las amenazas potenciales de violación de la protección de datos personales, siempre que se hayan enterado.
- 10.3. Dentro del marco de esta comunicación la persona que se haya enterado de un caso de violación de la protección de datos personales, o de una simple amenaza:
  - (a) describirá de la forma más completa y más precisa posible el carácter del caso sobre violación de la protección de datos personales o amenaza, incluyendo en lo posible, la categoría y el número aproximativo de sujetos de datos afectados, así como las categorías y la cantidad aproximativa de registros de datos personales afectados;
  - (b) describirá las probables consecuencias de la violación de la protección de datos personales;
  - (c) propondrá las posibles medidas a tomar con el fin de solucionar dicha violación de la protección de datos personales, eventualmente de atajar la amenaza en cuestión, incluyendo las eventuales medidas para atenuar los posibles impactos desfavorables.
- 10.4. Las personas obligadas por el presente Reglamento brindarán toda su colaboración para facilitar la toma de medidas adoptadas por la dirección de Aplatform en reacción a un caso de violación de la protección de datos personales o de amenaza.

## **11. DESTRUCCIÓN DE DOCUMENTOS**

- 11.1. Se procede a la destrucción de documentos sobre la base de:
  - i. Plazo vencido para la destrucción de los documentos según el esquema de retención;
  - ii. Desaparición de la razón, sobre la base de la que se establecieron los documentos conteniendo datos personales;
  - iii. Petición facultada del sujeto de datos de proceder a la cancelación.
- 11.2. En Aplatform los documentos son almacenados durante el plazo fijado por el esquema de retención. El plazo de destrucción de documentos se inicia el día 1 de enero del año siguiente después de haberse resuelta, elaborada o concluida la validez del documento. No se pueden acortar los plazos de destrucción de documentos. Excepcionalmente se puede prolongar el plazo de destrucción de documentos, siempre que Aplatform necesite el documento para su propia siguiente actividad.
- 11.3. En Aplatform los documentos llevan un código de destrucción que indica la manera de proceder una vez vencidos los plazos para la destrucción de los documentos:
  - (a) A – señala los documentos de valor durable, propuestos para su almacenamiento permanente;
  - (b) S – señala los documentos que pueden ser destruidos una vez vencido el plazo para su destrucción;
  - (c) V – señala los documentos que serán enjuiciados en procedimiento de destrucción de documentos y repartidos entre los documentos “A” o “S”;



(d)Z – señala los documentos que deben ser destruidos.

- 11.4. El procedimiento de destrucción de documentos se suele efectuar una vez al año de manera compleja para todo el instituto, siendo objeto del mismo todos los documentos, cuyos plazos de destrucción hayan vencido.
- 11.5. Al trabajador de Aplatform, responsable de la administración de documentos, le compete gestionar el proceso de destrucción de documentos. Elaborará la lista de documentos “A” y la lista de documentos “S; Z” (en cuanto a los documentos “V” el trabajador hará una selección previa y según el carácter de los mismos, los acoplará por separado a la lista de documentos “S; Z” o “A”), cuyo plazo de destrucción haya vencido. Luego añadirá la propuesta de destrucción a las listas creadas de esta manera.
- 11.6. Sobre la base de la propuesta de destrucción, una sociedad externa, respectivamente su representante autorizado para brindar dicho servicio, efectuará la inspección profesional de los documentos archivados propuestos para ser suprimidos. Una vez efectuado el proceso de destrucción de documentos se elaborará el protocolo sobre esta última que tendrá por contenido: la lista de documentos seleccionados como documentos de archivo, incluidos en su correspondiente categoría y lista de documentos que pueden ser destruidos. Forma parte inseparable del protocolo la información sobre el derecho del instituto a formular objeciones contra el resultado de la evaluación de los documentos. Al presentar una eventual objeción se iniciará el procedimiento administrativo.
- 11.7. Sobre la base de la autorización para destruir los documentos del grupo “S; Z” el trabajador responsable organizará la liquidación de los mismos de manera a que no se pueda abusar de las informaciones contenidas en los mismos.

## **12. COOPERACIÓN**

- 12.1. Con el fin de asegurar la conformidad con el GDPR, en caso de que sea necesario adaptar algunos procedimientos u operaciones realizadas en la actualidad y actividades que incluyen el almacenamiento y procesamiento de datos personales, o con el fin de hacer la evaluación de su influencia en la protección de datos personales, las personas relacionadas con el presente Reglamento tienen la obligación de brindar su indispensable cooperación y según las instrucciones colaborar con la persona responsable del procesamiento de datos personales en el instituto Aplatform.