## 1. INTRODUCCIÓN, ÁMBITO DE APLICACIÓN, DEFINICIONES

(1) Este contrato en https://mint-square.com regula los derechos y obligaciones del cliente y del contratista (en adelante denominados "partes") en el contexto del procesamiento de datos personales en nombre, a menos que se haya realizado un acuerdo separado entre las partes.

(2) Este contrato se aplica a todas las actividades en las que los empleados del contratista o los subcontratistas encargados por él procesan datos personales del cliente.

(3) Los términos utilizados en este contrato se entenderán de acuerdo con su definición en el Reglamento General de Protección de Datos (RGPD) de la UE. Cuando las declaraciones deban realizarse "por escrito" en lo sucesivo, se entiende la forma escrita según el § 126 BGB (Código Civil Alemán). De lo contrario, las declaraciones también pueden realizarse en otra forma, siempre que se asegure una verificabilidad adecuada.

(4) El servicio acordado contractualmente se presta exclusivamente en un Estado miembro de la Unión Europea o en un Estado contratante del Acuerdo sobre el Espacio Económico Europeo según la Cláusula Contractual Estándar. Cualquier otra prestación de servicios requiere el consentimiento previo del cliente y solo puede tener lugar si se cumplen los requisitos especiales de los artículos 44 y siguientes del RGPD (por ejemplo, decisión de adecuación de la Comisión, cláusulas de protección de datos estándar, códigos de conducta aprobados).

## 2. OBJETO, DURACIÓN Y ESPECIFICACIÓN DEL ENCARGO
### 2.1 Objeto

El cliente encarga al contratista la realización de servicios de publicidad en línea. Además, el cliente tiene la opción de obtener a través del contratista subcuentas de diversas Plataformas de Demanda (DSPs). A través de las DSPs, el cliente puede comprar medios digitales.

El procesamiento se basa en el contrato existente entre las partes (en adelante denominado "contrato principal"), que hace referencia a este acuerdo.

Para realizar el servicio de publicidad en línea, el contratista encarga diferentes plataformas tecnológicas como subempresas de servicios, que se nombran en el contrato principal y se enumeran bajo el ítem 6.

En particular, se realizarán las siguientes actividades de procesamiento para el cliente según sea necesario:

(1) ID de Cookie: Para vincular cada interacción individual con un dispositivo único, se genera una ID de dispositivo única para cada nuevo dispositivo, que interactúa con cualquier forma de publicidad DSP o herramientas de análisis de sitios web como Google Analytics. La ID única del dispositivo se almacena localmente en el navegador del usuario a través de una cookie. Dependiendo de la tecnología, la cookie expira no antes de 60 días y a más tardar un año (365 días) después de la última interacción. La ID del dispositivo se genera ya sea como un número aleatorio real o, en algunos casos, se combina con una ID generada a través de variables estáticas y dinámicas del navegador y la configuración del dispositivo.

a. En relación con la interacción de los usuarios con colocaciones publicitarias y medios digitales, como sitios web o aplicaciones móviles, se recopilan y almacenan ciertas informaciones para el cliente:

i. Navegadores utilizados por los usuarios y las configuraciones correspondientes.

ii. Información sobre el sistema operativo del dispositivo.

iii. Información sobre IDs de cookie y otras IDs asignadas a un dispositivo.

iv. Direcciones IP desde las cuales un dispositivo interactúa con el sitio web del cliente o una aplicación móvil; las direcciones IP pueden ser truncadas o encriptadas, o ambas, según las leyes locales u otros requisitos.

v. Información sobre la interacción y actividad de un usuario en sitios web y aplicaciones móviles, incluyendo el momento de la interacción

o actividad, las direcciones de internet involucradas y los términos de búsqueda introducidos en un motor de búsqueda.

vi. Información sobre la ubicación geográfica aproximada (ciudad, región, código postal) del dispositivo al acceder a un sitio web o una aplicación móvil, derivada de información de dirección IP truncada o datos GPS truncados.

vii. El subcontratista también puede recibir listas de IDs de cookie para habilitar publicidad dirigida y personalizada en sitios web y aplicaciones móviles. El subcontratista puede proporcionar estas IDs de cookie para uso de sus clientes a través del servicio, pero esto siempre se hará en conformidad con los permisos y restricciones impuestos por el tercero que proporciona los datos.

(2) ID de Publicidad Móvil: Las IDs de publicidad móvil son IDs técnicas en entornos de aplicaciones móviles, por ejemplo, en sistemas operativos de smartphones como Google Android y Apple iOS, que están bajo el control total del usuario y propietario del respectivo dispositivo y pueden ser restablecidas por el usuario a voluntad.

Las IDs de publicidad móvil pueden ser restablecidas por el usuario; ni MINT Square ni el subcontratista tienen control sobre una ID de publicidad móvil, ya que es asignada, cambiada y actualizada por el software del dispositivo del dispositivo final utilizado.

(3) IDs entre Dispositivos: Esta ID es una ID de usuario generada utilizando algoritmos estadísticos y probabilísticos para vincular dispositivos e identificadores del mismo usuario. También se utilizan IDs entre dispositivos de terceros, que se describen más detalladamente a continuación:

a. IDs de Socios: Las tecnologías DSP están conectadas con una variedad de socios como Google, Adobe, Oracle, Amazon y muchos otros. Para permitir la provisión de servicios DSP en el ecosistema publicitario basado en cookies, los DSPs intercambian automáticamente IDs pseudónimas con tales socios. La ID del socio expira no antes de 60 días pero a más tardar después de un año (365 días) después de la última interacción. Estas IDs están

estrictamente pseudonimizadas en ambos lados. La sincronización de IDs es un requisito esencial e ineludible para la provisión del servicio.

(4) Los DSPs no recopilan, usan o permiten al contratista transferir datos a la plataforma o usar datos en la plataforma que identifiquen directamente a una persona, como nombre, dirección, número de teléfono, dirección de correo electrónico o identificación gubernamental. Además, las plataformas DSP prohíben la recopilación, uso o transferencia de ciertas categorías de datos sensibles en la plataforma y utilizan soluciones técnicas para detectar datos directamente identificables en el servicio y tomar las medidas adecuadas. Para hacer cumplir este principio, las tecnologías DSP escanean activamente los datos en busca de infracciones.

## 2.2 Duración

El término de este contrato está regido por el término del contrato principal. El derecho a la terminación extraordinaria por causa justa permanece inafectado.

### 2.3 Especificación del Encargo

Este contrato se relaciona exclusivamente con los servicios de publicidad en línea.
En particular, las operaciones de procesamiento enumeradas bajo el ítem 2.1 pueden realizarse a través de las plataformas DSP.

## 3. OBLIGACIONES DEL CONTRATISTA

(1) El contratista solo puede procesar datos de personas afectadas dentro del ámbito del encargo y las instrucciones del cliente, a menos que exista un caso excepcional en el sentido del Artículo 28 (3) a) del RGPD. Las instrucciones se definen inicialmente por este contrato y el contrato principal y pueden ser cambiadas, complementadas o reemplazadas por instrucciones individuales del cliente en forma escrita o en un formato electrónico (forma de texto) al lugar designado por el contratista (instrucción individual). Las instrucciones no previstas en el contrato se tratan como una solicitud de cambio de servicio. Las instrucciones orales deben ser confirmadas por escrito o en forma de texto sin demora. El contratista informa al cliente inmediatamente si considera que una instrucción viola las leyes aplicables. El contratista puede suspender la

implementación de la instrucción hasta que sea confirmada o modificada por el cliente.

(2) Si el contratista está legalmente obligado a un procesamiento específico, informará al cliente de esto antes del procesamiento, a menos que la notificación esté legalmente prohibida. Además, el contratista no utiliza los datos proporcionados para la ejecución de los servicios de publicidad en línea para otros fines, especialmente no para sus propios fines.

(3) El contratista diseñará su organización interna dentro de su área de responsabilidad para cumplir con los requisitos especiales de protección de datos.

(4) Implementará medidas técnicas y organizativas para proteger adecuadamente los datos del cliente que cumplan con los requisitos del Reglamento General de Protección de Datos (Art. 32 RGPD). El contratista debe implementar medidas técnicas y organizativas que aseguren la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios relacionados con el procesamiento de manera permanente. Las medidas técnicas y organizativas del contratista se especifican al final del contrato. El cliente es responsable de asegurar que estas proporcionen un nivel de protección adecuado para los riesgos de los datos que se procesan. Un cambio en las medidas de seguridad tomadas queda reservado para el contratista, pero debe asegurarse de que no se reduzca el nivel de protección acordado contractualmente. El contratista asegura que los datos procesados en nombre del cliente se mantengan estrictamente separados de otros conjuntos de datos.

(5) El contratista proporciona prueba regular del cumplimiento de sus obligaciones, en particular de la implementación completa de las medidas técnicas y organizativas acordadas y su efectividad.

(6) El contratista asegura el cumplimiento de sus obligaciones según el Art. 32 (1) lit. d) del RGPD, de utilizar un procedimiento para revisar regularmente la efectividad de las medidas técnicas y organizativas para asegurar la seguridad del procesamiento.

(7) El contratista asegura que está prohibido para los empleados y otras personas que trabajan para el contratista procesar los datos fuera de la instrucción. Además, el contratista asegura que las personas autorizadas para

procesar datos personales se han comprometido a la confidencialidad o están sujetas a una obligación legal de confidencialidad adecuada. La obligación de confidencialidad/secreto también continúa después de la finalización del encargo.

(8) En relación con el procesamiento encargado, el contratista apoya al cliente en la creación y actualización del directorio de actividades de procesamiento y en la realización de la evaluación de impacto de protección de datos. Toda la información y documentación necesaria debe ser mantenida y proporcionada al cliente a petición de inmediato.

(9) El contratista solo puede proporcionar información a terceros o al sujeto de datos con el consentimiento previo del cliente. En la medida acordada, el contratista apoya al cliente dentro de sus capacidades para cumplir con las solicitudes y reclamaciones de las personas afectadas según el Capítulo III del RGPD, así como para cumplir con las obligaciones mencionadas en los artículos 33 a 36 del RGPD. En el caso de una reclamación de una persona afectada contra el cliente con respecto a posibles reclamaciones según el Art. 82 del RGPD, el contratista se compromete a apoyar al cliente en la defensa de la reclamación dentro de sus capacidades. Si una persona afectada se dirige al contratista con solicitudes de corrección, eliminación o información, el contratista referirá inmediatamente a la persona afectada al cliente, siempre que se pueda asignar al cliente según la información de la persona afectada (ver Capítulo 7).

(10) El contratista informa al cliente inmediatamente sobre violaciones de la protección de datos personales. También deben informarse casos sospechosos. La notificación debe realizarse a más tardar dentro de las 24 horas después de que el contratista se entere del evento relevante al delegado de protección de datos del cliente. Debe contener al menos la siguiente información:

a. una descripción de la naturaleza de la violación de la protección de datos personales, si es posible con indicación de las categorías y el número aproximado de personas afectadas, las categorías afectadas y el número aproximado de registros de datos personales afectados;
b. el nombre y los datos de contacto del delegado de protección de datos u otro punto de contacto para obtener más información;
c. una descripción de las consecuencias probables de la violación de la protección de datos personales;

d. una descripción de las medidas tomadas o propuestas por el contratista para abordar la violación de la protección de datos personales y, si es aplicable, medidas para mitigar sus posibles efectos adversos.

(11) También deben informarse inmediatamente interrupciones significativas en la finalización del encargo, así como violaciones del contratista o de las personas empleadas por él contra las disposiciones de protección de datos o las disposiciones tomadas en este contrato.

(12) Si el cliente es sometido a un control por parte de autoridades de supervisión u otros órganos o si las personas afectadas ejercen derechos contra él, el contratista se compromete a apoyar al cliente en la medida necesaria, en la medida en que el procesamiento por encargo esté involucrado. El contratista informa inmediatamente al cliente de controles o medidas de autoridades de supervisión u otros terceros, en la medida en que estos tengan referencias al procesamiento por encargo.

(13) El procesamiento por encargo se lleva a cabo exclusivamente dentro de la UE o el EEE. Cualquier traslado a un tercer país solo puede tener lugar con el consentimiento del cliente y bajo las condiciones contenidas en el Reglamento General de Protección de Datos, así como en cumplimiento de las disposiciones de este contrato.

(14) Si el contratista no está establecido en la Unión Europea, designa a una persona de contacto responsable en la Unión Europea según el Art. 27 del Reglamento General de Protección de Datos. Los datos de contacto de la persona de contacto y cualquier cambio en la persona del contacto deben comunicarse al cliente inmediatamente. Si el contratista utiliza proveedores de servicios ubicados fuera del ámbito de aplicación del RGPD, el contratista explica completamente cómo se asegura el cumplimiento del RGPD, a menos que el servicio sea proporcionado por una empresa bajo la Cláusula Contractual Estándar.

(15) El contratista corrige o elimina los datos relacionados con el contrato si el cliente lo instruye y esto está cubierto por el marco de instrucción (ver Capítulo 2.3). Otras disposiciones sobre la eliminación se contienen en el Capítulo 7.

(16) Los datos de contacto del delegado de protección de datos en el procesador de datos son:

Kleinermann & Sohn GmbH
Stefan Kleinermann
+49 (0) 2401 60 540
info@das-datenschutz-team.de

## 4. OBLIGACIONES DEL CLIENTE

(1) El cliente debe informar al contratista de inmediato y completamente si detecta errores o irregularidades con respecto a las disposiciones de protección de datos en los resultados del encargo.

(2) En caso de una reclamación contra el cliente por una persona afectada con respecto a posibles reclamaciones según el Art. 82 del RGPD, se aplica el §3 párr. 10 en consecuencia.

(3) El cliente nombra a la persona de contacto para cuestiones de protección de datos que surjan en el contexto del contrato al contratista. El contratista nombra al delegado de protección de datos (DPD) con sus datos de contacto para el manejo de cuestiones de protección de datos y preocupaciones que surjan en el contexto del contrato al cliente.

## 5. POSIBILIDADES DE PRUEBA

El contratista proporciona prueba del cumplimiento de las obligaciones establecidas en este contrato con medios adecuados al cliente. El cliente y el contratista acuerdan que la prueba se proporciona mediante la realización de una autoauditoría/inspección utilizando un cuestionario.

## 6. SUBCONTRATISTAS (RELACIONES DE SUBPROCESAMIENTO)

(1) Los servicios acordados contractualmente o los siguientes servicios parciales descritos se llevan a cabo con la implicación de los siguientes subcontratistas:

- ADFORM A/S
  Dirección:
  Silkegade 3B, DK-1113 Copenhague, Dinamarca

  URL:
  www.adform.com

  Servicio:
  Proveedor de servicios publicitarios técnicos

  Lugar de procesamiento de datos:
  Dinamarca

- VIRTUAL MINDS GMBH
  Dirección:
  Ellen-Gottlieb-Str. 16 D-79106 Friburgo de Brisgovia, Alemania

  URL:
  www.virtualminds.de

  Servicio:
  Proveedor de servicios publicitarios técnicos

  Lugar de procesamiento de datos:
  Alemania

- THE UK TRADE DESK LTD.
  Dirección:
  10th Floor, 1 Bartholomew Close Londres EC1A 7BL Reino Unido

  URL:
  www.thetradedesk.com

  Servicio:
  Proveedor de servicios publicitarios técnicos

Lugar de procesamiento de datos:
EE. UU. según la Cláusula Contractual Estándar

(2) La comisión de subcontratistas solo está permitida con el consentimiento escrito del cliente en casos individuales.

(3) Existe una relación de subcontratista que requiere consentimiento si el contratista comisiona a otros contratistas para todo o parte del servicio acordado en el contrato. El contratista hará acuerdos con estos terceros en la medida necesaria para asegurar medidas adecuadas de protección de datos y seguridad de la información.

(4) El contratista informa al cliente por escrito sobre la implicación de subcontratistas adicionales o la sustitución de subcontratistas listados. El cliente no puede oponerse a esta solicitud sin un motivo válido de protección de datos.

(5) Si el contratista otorga órdenes a subcontratistas, es responsabilidad del contratista transferir sus obligaciones de protección de datos de este contrato al subcontratista.

(6) La comisión de subcontratistas que no realizan procesamientos exclusivamente desde el territorio de la UE o el EEE es posible solo bajo las condiciones mencionadas en el Capítulo 3 (13) y (14) de este contrato. Es particularmente permitido en la medida en que y mientras el subcontratista ofrezca garantías adecuadas de protección de datos. El contratista informa al cliente sobre las garantías de protección de datos específicas ofrecidas por el subcontratista y cómo se puede obtener una prueba de ello.

(7) Las relaciones de subcontratación en el sentido de este contrato son solo aquellos servicios que tienen una conexión directa con la prestación del servicio principal. Los servicios auxiliares, como el transporte y la limpieza, así como el uso de servicios de telecomunicaciones o servicio al usuario, no están incluidos. La obligación del contratista de asegurar el cumplimiento de la protección de datos y la seguridad de los datos también en estos casos permanece inalterada.

## 7. REGULACIONES SOBRE LA CORRECCIÓN, ELIMINACIÓN Y BLOQUEO DE DATOS

(1) Los datos procesados en el marco del encargo solo serán corregidos, eliminados o bloqueados por el contratista de acuerdo con el acuerdo contractual y siguiendo las instrucciones del cliente (ver Capítulo 2.3).

(2) El contratista cumplirá siempre con las instrucciones correspondientes del cliente, incluso más allá de la finalización de este contrato.

(3) Si no es posible una eliminación conforme a la protección de datos o una restricción correspondiente del procesamiento de datos, el contratista asume la destrucción conforme a la protección de datos de soportes de datos y otros materiales en base a un encargo individual del cliente o devuelve estos soportes de datos al cliente, a menos que ya esté acordado en el contrato. En casos especiales determinados por el cliente, se realiza un almacenamiento o entrega. La compensación y las medidas de protección se acordarán por separado, a menos que ya estén acordadas en el contrato.

(4) No se crearán copias o duplicados sin el conocimiento del cliente. Las excepciones son duplicaciones temporalmente necesarias por razones técnicas, en la medida en que se excluya un deterioro del nivel de protección de datos acordado aquí.

(5) Los soportes de datos dedicados provenientes del cliente o utilizados para el cliente se marcarán de manera especial y estarán sujetos a una gestión continua. Deben almacenarse de manera adecuada en todo momento y no deben ser accesibles a personas no autorizadas. Las entradas y salidas se documentan.

(6) Al final de la relación contractual o en cualquier momento a petición del cliente, el contratista debe destruir los datos procesados en el encargo, los soportes de datos y todos los demás materiales según la elección del cliente o entregarlos al cliente. También deben destruirse todas las copias existentes de los datos. La destrucción debe realizarse de tal manera que la restauración incluso de información residual con un esfuerzo razonable ya no sea posible.

(7) El contratista está obligado a asegurar la devolución o eliminación inmediata también en los subcontratistas.

(8) El contratista debe proporcionar prueba de la destrucción adecuada y presentarla inmediatamente al cliente.

(9) Las documentaciones que sirven como prueba de un procesamiento adecuado de los datos deben ser conservadas por el contratista de acuerdo con los respectivos plazos de retención incluso más allá del final del contrato. Puede entregarlas al cliente al final del contrato para su descarga.

Tenga en cuenta: Esta traducción se proporciona solo para fines de conveniencia. La versión alemana de este documento es la versión legalmente vinculante ya que la empresa está basada en Alemania.

## MEDIDAS TÉCNICAS Y ORGANIZATIVAS (MTO) PARA LA PROTECCIÓN DE DATOS

PSEUDONIMIZACIÓN (ART. 32 (1) LIT. A RGPD; ART. 25 (1) RGPD)
El procesamiento de datos personales de tal manera que los datos ya no puedan ser atribuidos a un sujeto de datos específico sin la utilización de información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas.

### 1. PSEUDONIMIZACIÓN / MEDIDAS TÉCNICAS-ORGANIZATIVAS – ESPECÍFICAS DEL PROYECTO

Detalles/Observaciones:
Los datos de las cookies no pueden ser asignados a una persona específica. La pseudonimización de los datos se lleva a cabo a través de los subproveedores de servicios. Por lo tanto, los subproveedores de servicios aseguran que las cookies no puedan ser atribuidas a una persona específica.

### 2. CONFIDENCIALIDAD (ART. 32 (1) LIT. B RGPD)

La capacidad de asegurar la confidencialidad de los sistemas y servicios relacionados con el procesamiento de manera permanente.

**2.1 Control de Acceso** – Impedir el acceso no autorizado a las instalaciones de procesamiento de datos, por ejemplo:

- Medidas adecuadas para negar a personas no autorizadas el acceso a las instalaciones de procesamiento de datos donde se procesan o utilizan datos personales.

- Control de Acceso

- Llaves de seguridad magnéticas personalizadas: Cada empleado recibe una llave de seguridad magnética personal que controla el acceso a nuestras instalaciones. Esta llave es única y asignada individualmente para asegurar que solo las personas autorizadas tengan acceso a áreas sensibles. La pérdida o transferencia de llaves de seguridad a terceros debe ser reportada inmediatamente, y se toman medidas adecuadas (desactivación de la llave) para mantener la seguridad.

  2.2 Control de Acceso – Sin uso no autorizado del sistema, por ejemplo:

- Medidas adecuadas para prevenir que los sistemas de procesamiento de datos puedan ser utilizados por personas no autorizadas.

- Control de Acceso / Sistemas Técnicos – Medidas Básicas

- El acceso a los sistemas informáticos solo es posible con contraseña.
- Los mecanismos de bloqueo automático de los sistemas informáticos están habilitados a través de Microsoft Cloud 365.
- Las actualizaciones del sistema se realizan automáticamente.
- Todos los sistemas informáticos están equipados con software antivirus / firewall.
- Los clientes mismos asignan contraseñas, que pueden ser cambiadas después de la puesta en marcha inicial y no son conocidas por el contratista.
- Cada 91 días se emite un recordatorio automático de que las contraseñas deben ser cambiadas por el usuario.

  2.3 Control de Acceso

- Medidas que aseguran que las personas autorizadas a utilizar un sistema de procesamiento de datos solo puedan acceder a los datos a los que su autorización de acceso se aplica, y que los datos personales no puedan ser leídos, copiados, modificados o eliminados sin autorización durante el procesamiento, el uso y después del almacenamiento.

- Implementación de un concepto de autorización, donde a cada cliente se le asigna acceso solo a su propia área de inicio de sesión y datos de campaña;
- Registro de cambios en los archivos de registro;
- Solo el personal funcional tiene acceso a todos los datos de clientes y campañas.
- Los empleados tienen derechos de acceso individuales según sus necesidades.
- Control de separación asegurando que los datos de los clientes se almacenen separadamente de manera lógica de otros datos.

## 3. INTEGRIDAD (ART. 32 (1) LIT. B RGPD)

La capacidad de asegurar la integridad de los sistemas y servicios relacionados con el procesamiento de manera permanente (protección contra la modificación o eliminación no autorizadas durante el almacenamiento electrónico, la transmisión o el transporte), por ejemplo:

- Los datos pueden ser ingresados y procesados por el cliente y, dependiendo del pedido, también por el contratista.
- El acceso por parte del cliente se registra.
- Cuentas de correo electrónico cifradas.

## 4. DISPONIBILIDAD Y RESILIENCIA (ART. 32 (1) LIT. B RGPD)

La capacidad de asegurar la disponibilidad y resiliencia de los sistemas y servicios relacionados con el procesamiento de manera permanente (protección contra la destrucción o pérdida accidental o intencionada), por ejemplo:

- Los datos de las campañas también están asegurados por nuestros subproveedores de servicios.

## 5. RESTAURACIÓN RÁPIDA (ART. 32 (1) LIT. C RGPD)

La capacidad de restaurar rápidamente la disponibilidad de los datos personales y el acceso a ellos en caso de un incidente físico o técnico, por ejemplo:

- En caso de que se haya producido o identificado una pérdida de datos, se informa a la dirección. Para los datos de las campañas, se informa al

subproveedor de servicios, que restaura los datos a través de los sistemas de copia de seguridad.

## 6. PROCEDIMIENTOS DE REVISIÓN, EVALUACIÓN Y EVALUACIÓN REGULARES (ART. 32 (1) LIT. D RGPD; ART. 25 (1) RGPD)

Debe existir un procedimiento para la revisión, evaluación y evaluación regulares de la efectividad de las medidas técnicas y organizativas para asegurar la seguridad del procesamiento, por ejemplo:

- Los empleados de MINT Square reciben formación regular en derecho de protección de datos y están familiarizados con las instrucciones procesales y las directrices de uso para el procesamiento de datos en nombre, incluyendo el derecho de instrucción del cliente.
- Cada empleado está obligado a cumplir con los requisitos de protección de datos según el RGPD a más tardar el primer día de su actividad.
- Existe un registro de procesamiento en el sentido del Art. 30 (1), (2) RGPD y un proceso para la evaluación de impacto (DSFA), que se realiza regularmente.

## 7. CONFIGURACIONES PREDETERMINADAS FAVORABLES A LA PROTECCIÓN DE DATOS (ART. 25 (2) RGPD)

El responsable del tratamiento toma medidas técnicas y organizativas adecuadas para garantizar que, por defecto, solo se procesen los datos personales necesarios para cada finalidad específica del procesamiento.

- Se recopila información de cookies
- MINT Square utiliza cookies de navegador a través del subproveedor de servicios para almacenar información sobre las preferencias de los visitantes del sitio web, como la exclusión voluntaria y la ID única del navegador del visitante, y para almacenar información sobre la funcionalidad del servidor de anuncios del subproveedor de servicios – límite de frecuencia, rotación de anuncios, atribución de medios post-clic.
- El subproveedor de servicios lee las cookies del navegador en cada solicitud HTTP-GET al servidor y pasa la ID del navegador del visitante o información de que las cookies están desactivadas o que el visitante ha sido excluido del servicio por el proveedor en cada transacción – impresión, clic, visita al sitio web, otro evento.

- Los subproveedores de servicios solo colocan cookies en el navegador del visitante cuando tiene sentido – se utilizaron algunas funciones del servidor de anuncios o para extender la vida útil de las cookies.
- Los subproveedores de servicios no utilizan otras cookies (por ejemplo, cookies Flash) o funciones similares para rastrear al visitante o al navegador del visitante. Los subproveedores de servicios no almacenan ninguna información privada o sensible en las cookies del navegador.