MINT Square DPA+TOMs | Traduction en français

Statut : 2021-09-20

1. INTRODUCTION, CHAMP D'APPLICATION, DÉFINITIONS

(1) Ce contrat sur https://mint-square.com régit les droits et obligations du client et du contractant (ci-après désignés par « parties ») dans le cadre du traitement des données personnelles pour le compte, sauf si un accord séparé a été conclu entre les parties.

(2) Ce contrat s'applique à toutes les activités dans lesquelles les employés du contractant ou les sous-traitants commissionnés par lui traitent des données personnelles du client.

(3) Les termes utilisés dans ce contrat doivent être compris conformément à leur définition dans le Règlement Général sur la Protection des Données (RGPD) de l'Union européenne. Lorsque les déclarations doivent être faites « par écrit » dans ce qui suit, la forme écrite selon le § 126 BGB (Code civil allemand) est prévue. Par aillleurs, les déclarations peuvent également être faites sous une autre forme, pourvu qu'une vérifiabilité adéquate soit assurée.

(4) Le service contractuellement convenu est fourni exclusivement dans un État membre de l'Union européenne ou dans un État contractant de l'accord sur l'Espace économique européen selon la Clause contractuelle standard. Toute autre prestation de services nécessite le consentement préalable du client et ne peut avoir lieu que si les conditions spéciales des articles 44 et ss. RGPD sont remplies (par exemple, décision d'adéquation de la Commission, clauses standard de protection des données, codes de conduite approuvés).

2. OBJET, DURÉE ET SPÉCIFICATION DE LA MISSION

2.1 Objet

Le client charge le contractant de réaliser des services de publicité en ligne. En outre, le client a la possibilité d'obtenir via le contractant des sous-comptes de différentes Plateformes d'Achat (DSPs). À travers les DSPs, le client peut acheter des médias numériques.

Le traitement est basé sur le contrat existant entre les parties (ci-après désigné par « contrat principal »), qui fait référence à cet accord.

Pour réaliser le service de publicité en ligne, le contractant commissionne différentes plateformes technologiques en tant que sous-services, qui sont nommées dans le contrat principal et répertoriées sous l'article 6.

En particulier, les activités de traitement suivantes seront effectuées pour le client selon les besoins :

(1) Cookie-ID : Pour lier chaque interaction individuelle avec un seul appareil, un identifiant d'appareil unique est généré pour chaque nouvel appareil, qui interagit avec toute forme de publicité DSP ou des outils d'analyse de site web tels que Google Analytics. L'identifiant unique de l'appareil est stocké localement dans le navigateur de l'utilisateur via un cookie. Selon la technologie, le cookie expire au plus tôt 60 jours et au plus tard un an (365 jours) après la dernière interaction. L'identifiant de l'appareil est soit généré comme un véritable nombre aléatoire, soit, dans certains cas, combiné avec un identifiant généré à travers des variables statiques et dynamiques du navigateur et de la configuration de l'appareil.

a. En lien avec l'interaction des utilisateurs avec des placements publicitaires et des médias numériques, tels que les sites web ou les applications mobiles, certaines informations sont collectées et stockées pour le client :

i. Navigateurs utilisés par les utilisateurs et les paramètres correspondants.

ii. Informations sur le système d'exploitation de l'appareil.

iii. Informations sur les identifiants de cookie et autres identifiants attribués à un appareil.

iv. Adresses IP à partir desquelles un appareil interagit avec le site web du client ou une application mobile ; les adresses IP peuvent être tronquées ou cryptées, ou les deux, en fonction des lois locales ou d'autres exigences.

v. Informations sur l'interaction et l'activité d'un utilisateur sur les sites web et applications mobiles, y compris le moment de l'interaction ou de l'activité, les adresses Internet impliquées et les termes de recherche saisis dans un moteur de recherche.

vi. Informations sur l'emplacement géographique approximatif (ville, région, code postal) de l'appareil lorsqu'il accède à un site web ou à une

application mobile, dérivées d'informations d'adresse IP tronquées ou de données GPS tronquées.

vii. Le sous-traitant peut également recevoir des listes d'identifiants de cookie pour permettre une publicité ciblée et personnalisée sur les sites web et applications mobiles. Le sous-traitant peut fournir ces identifiants de cookie pour utilisation par ses clients via le service, mais cela sera toujours fait en conformité avec les autorisations et restrictions imposées par le tiers fournissant les données.

(2) Identifiant de publicité mobile : Les identifiants de publicité mobile sont des identifiants techniques dans les environnements d'application mobile, par exemple, sur les systèmes d'exploitation de smartphones tels que Google Android et Apple iOS, qui sont sous le plein contrôle de l'utilisateur et propriétaire du dispositif respectif et peuvent être réinitialisés par l'utilisateur à volonté.

Les identifiants de publicité mobile peuvent être réinitialisés par l'utilisateur ; ni MINT Square, ni le sous-traitant n'ont de contrôle sur un identifiant de publicité mobile, car il est attribué, modifié et mis à jour par le logiciel de l'appareil de l'appareil final utilisé.

(3) Identifiants multi-appareils : Cet identifiant est un identifiant d'utilisateur généré en utilisant des algorithmes statistiques et probabilistes pour lier des appareils et des identificateurs du même utilisateur. Des identifiants multi-appareils de tiers sont également utilisés, qui sont décrits plus en détail ci-dessous :

a. Identifiants de partenaires : Les technologies DSP sont connectées avec une variété de partenaires comme Google, Adobe, Oracle, Amazon et bien d'autres. Pour permettre la fourniture des services DSP dans l'écosystème publicitaire basé sur les cookies, les DSPs échangent automatiquement des identifiants pseudonymes avec de tels partenaires. L'identifiant de partenaire expire au plus tôt 60 jours mais au plus tard après un an (365 jours) après la dernière interaction. Ces identifiants sont strictement pseudonymisés des deux côtés. La synchronisation des identifiants est une condition essentielle et incontournable pour la fourniture du service.

(4) Les DSPs ne collectent, n'utilisent ou ne permettent pas au contractant de transférer des données sur la plateforme ou d'utiliser des données sur la plateforme qui identifient directement une personne, telles que le nom, l'adresse,

le numéro de téléphone, l'adresse e-mail ou l'identification gouvernementale. En outre, les plateformes DSP interdisent la collecte, l'utilisation ou le transfert de certaines catégories de données sensibles sur la plateforme et utilisent des solutions techniques pour détecter des données directement identifiables dans le service et prendre des mesures appropriées. Pour faire respecter ce principe, les technologies DSP scannent activement les données pour détecter les violations.

2.2 Durée

La durée de ce contrat est régie par la durée du contrat principal. Le droit de résiliation extraordinaire pour motif valable reste inchangé.

2.3 Spécification de la mission

Cet accord concerne exclusivement les services de publicité en ligne.
En particulier, les opérations de traitement énumérées sous l'article 2.1 peuvent être réalisées via les plateformes DSP.

3. OBLIGATIONS DU CONTRACTANT

(1) Le contractant ne peut traiter les données des personnes concernées que dans le cadre de la mission et des instructions du client, sauf s'il existe un cas exceptionnel au sens de l'article 28 (3) a) du RGPD. Les instructions sont initialement définies par cet accord et le contrat principal et peuvent être modifiées, complétées ou remplacées par des instructions individuelles du client sous forme écrite ou sous un format électronique (forme de texte) à l'endroit désigné par le contractant (instruction individuelle). Les instructions non prévues dans le contrat sont traitées comme une demande de modification de la prestation. Les instructions orales doivent être confirmées par écrit ou sous forme de texte sans délai. Le contractant informe le client immédiatement s'il estime qu'une instruction viole les lois applicables. Le contractant peut suspendre la mise en œuvre de l'instruction jusqu'à ce qu'elle soit confirmée ou modifiée par le client.

(2) Si le contractant est légalement obligé à un traitement spécifique, le contractant en informe le client avant le traitement, sauf si la notification est légalement interdite. En outre, le contractant n'utilise pas les données fournies pour l'exécution des services de publicité en ligne à d'autres fins, notamment pas à ses propres fins.

(3) Le contractant concevra son organisation interne dans son domaine de responsabilité pour répondre aux exigences spéciales de la protection des données.

(4) Seront mises en œuvre des mesures techniques et organisationnelles visant à protéger de manière adéquate les données du client et répondant aux exigences du règlement général sur la protection des données (article 32 du RGPD). Le contractant doit implémenter des mesures techniques et organisationnelles qui garantissent la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services liés au traitement de manière permanente. Les mesures techniques et organisationnelles du contractant sont précisées à la fin du contrat. Le client est responsable de s'assurer que celles-ci offrent un niveau de protection adéquat pour les risques des données traitées. Un changement des mesures de sécurité prises reste réservé au contractant, mais il doit être assuré que le niveau de protection convenu contractuellement n'est pas réduit. Le contractant assure que les données traitées pour le compte du client sont strictement séparées des autres ensembles de données.

(5) Le contractant fournit la preuve régulière du respect de ses obligations, en particulier de la mise en œuvre complète des mesures techniques et organisationnelles convenues et de leur efficacité.

(6) Le contractant garantit le respect de ses obligations en vertu de l'Art. 32 (1) lit. d) du RGPD, d'utiliser une procédure pour réviser régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

(7) Le contractant garantit qu'il est interdit aux employés et autres personnes travaillant pour le contractant de traiter les données en dehors de l'instruction. En outre, le contractant garantit que les personnes autorisées à traiter les données personnelles se sont engagées à respecter la confidentialité ou sont soumises à une obligation légale de confidentialité appropriée. L'obligation de confidentialité / de discrétion continue également après la fin de la mission.

(8) Dans le cadre du traitement commandé, le contractant soutient le client dans la création et la mise à jour du répertoire des activités de traitement et dans la réalisation de l'évaluation d'impact sur la protection des données. Toutes les informations et documentations nécessaires doivent être conservées et fournies au client sur demande immédiatement.

(9) Le contractant ne peut fournir des informations à des tiers ou à la personne concernée qu'avec le consentement préalable du client. Dans la mesure convenue, le contractant soutient le client dans la mesure de ses capacités pour répondre aux demandes et réclamations des personnes concernées conformément au Chapitre III du RGPD ainsi que pour respecter les obligations mentionnées dans les articles 33 à 36 du RGPD. En cas de réclamation d'une personne concernée contre le client concernant des réclamations possibles en vertu de l'art. 82 du RGPD, le contractant s'engage à

soutenir le client dans la défense de la réclamation dans la mesure de ses capacités. Si une personne concernée adresse au contractant des demandes de correction, de suppression ou d'information, le contractant réfère immédiatement la personne concernée au client, pourvu qu'une attribution au client soit possible sur la base des informations de la personne concernée (voir Chapitre 7).

(10) Le contractant informe le client immédiatement des violations de la protection des données personnelles. Les cas suspects doivent également être signalés. La notification doit être faite au plus tard dans les 24 heures après que le contractant a pris connaissance de l'événement pertinent au délégué à la protection des données du client. Elle doit contenir au moins les informations suivantes :

a. une description de la nature de la violation de la protection des données personnelles, si possible avec indication des catégories et du nombre approximatif de personnes concernées, des catégories touchées et du nombre approximatif de dossiers de données personnelles concernés;

b. le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact pour plus d'informations ;

c. une description des conséquences probables de la violation de la protection des données personnelles ;

d. une description des mesures prises ou proposées par le contractant pour remédier à la violation de la protection des données personnelles et, le cas échéant, des mesures pour atténuer ses effets négatifs possibles.

(11) Les perturbations importantes dans l'exécution de la mission ainsi que les violations par le contractant ou les personnes qu'il emploie des lois sur la protection des données ou des dispositions prévues dans le présent contrat doivent également être signalées immédiatement.

(12) Si le client est soumis à un contrôle par les autorités de surveillance ou d'autres instances ou si des personnes concernées font valoir des droits contre lui, le contractant s'engage à soutenir le client dans la mesure nécessaire, dans la mesure où le traitement du compte est concerné. Le contractant informe immédiatement le client des contrôles ou des mesures des autorités de surveillance ou d'autres tiers, dans la mesure où ceux-ci se réfèrent au traitement du contrat.

(13) Le traitement contractuel est effectué exclusivement dans l'UE ou l'EEE. Tout transfert dans un pays tiers ne peut avoir lieu qu'avec le consentement du client et dans

le respect des conditions contenues dans le Règlement Général sur la Protection des Données ainsi que dans le respect des dispositions de ce contrat.

(14) Si le contractant n'est pas établi dans l'Union européenne, il désigne une personne de contact responsable dans l'Union européenne conformément à l'Art. 27 du Règlement Général sur la Protection des Données. Les coordonnées de la personne de contact et tout changement de personne de contact doivent être communiqués au client immédiatement. Si le contractant utilise des prestataires de services situés en dehors du champ d'application du RGPD, il explique en détail comment la conformité au GDPR est assurée, à moins que le service ne soit fourni par une société en vertu de la Clause contractuelle standard.

(15) Le contractant corrige ou supprime les données relatives au contrat si le client le demande et cela est couvert par le cadre d'instruction (voir Chapitre 2.3). D'autres dispositions sur la suppression sont contenues dans le Chapitre 7.

(16) Les coordonnées du délégué à la protection des données chez le processeur de données sont :

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

4. OBLIGATIONS DU CLIENT

(1) Le client doit informer le contractant immédiatement et complètement s'il détecte des erreurs ou des irrégularités concernant les dispositions de protection des données dans les résultats de la commande.

(2) En cas de réclamation contre le client par une personne concernée concernant des réclamations possibles en vertu de l'art. 82 du RGPD, l'§3 al. 10 s'applique en conséquence.

(3) Le client nomme la personne de contact pour les questions de protection des données survenant dans le cadre du contrat au contractant. Le contractant nomme le délégué à la protection des données (DPO) avec ses coordonnées pour le traitement des questions de protection des données et des préoccupations survenant dans le cadre du contrat au client.

5. POSSIBILITÉS DE PREUVE

Le contractant fournit la preuve du respect des obligations établies dans ce contrat par des moyens appropriés au client. Le client et le contractant conviennent que la preuve est fournie par la réalisation d'un auto-audit / inspection à l'aide d'un questionnaire.

6. SOUS-TRAITANTS (RELATIONS DE SOUS-TRAITANCE)

(1) Les services convenus contractuellement ou les services partiels suivants décrits sont réalisés avec l'implication des sous-traitants suivants :

- ADFORM A/S
  Adresse :
  Silkegade 3B, DK-1113 Copenhague, Danemark

  URL :
  www.adform.com

  Service :
  Fournisseur de services publicitaires techniques

  Lieu de traitement des données :
  Danemark

- VIRTUAL MINDS GMBH
  Adresse :
  Ellen-Gottlieb-Str. 16 D-79106 Fribourg-en-Brisgau, Allemagne

  URL :
  www.virtualminds.de

  Service :
  Fournisseur de services publicitaires techniques

  Lieu de traitement des données :
  Allemagne

- THE UK TRADE DESK LTD.
  Adresse :
  10th Floor, 1 Bartholomew Close Londres EC1A 7BL Royaume-Uni

URL :
www.thetradedesk.com

Service :
Fournisseur de services publicitaires techniques

Lieu de traitement des données :
USA selon la Clause contractuelle standard

(2) La commission de sous-traitants n'est autorisée qu'avec le consentement écrit du client dans des cas individuels.

(3) Une relation de sous-traitance nécessitant un consentement existe si le contractant commissionne d'autres contractants pour l'ensemble ou une partie du service convenu dans le contrat. Le contractant conclura des accords avec ces tiers dans la mesure nécessaire pour assurer des mesures de protection des données et de sécurité de l'information appropriées.

(4) Le contractant informe le client par écrit de l'implication de sous-traitants supplémentaires ou du remplacement des sous-traitants répertoriés. Le client ne peut pas s'opposer à cette demande sans motif valable de protection des données.

(5) Si le contractant confie des commandes à des sous-traitants, il incombe au contractant de transférer ses obligations en matière de protection des données de ce contrat au sous-traitant.

(6) Le recours à des sous-traitants qui n'assurent pas exclusivement le traitement à partir du territoire de l'UE ou de l'EEE n'est possible que dans les conditions mentionnées au chapitre 3, points 13 et 14, du présent contrat. Il est notamment autorisée dans la mesure où et aussi longtemps que le sous-traitant offre des garanties de protection des données adéquates. Le contractant informe le client des garanties spécifiques de protection des données offertes par le sous-traitant et de la manière dont il est possible d'en obtenir la preuve.

(7) Les relations de sous-traitance au sens du présent contrat sont uniquement les services qui ont un lien direct avec la prestation du service principal. Les services auxiliaires, tels que le transport et le nettoyage, ainsi que l'utilisation de services de télécommunications ou de services aux utilisateurs, ne sont pas inclus. L'obligation du contractant de veiller au respect de la protection et de la sécurité des données reste inchangée dans ces cas.

7. RÉGLEMENTATIONS SUR LA CORRECTION, LA SUPPRESSION ET LE BLOCAGE DES DONNÉES

(1) Les données traitées dans le cadre de la commande ne seront corrigées, supprimées ou bloquées par le contractant que conformément à l'accord contractuel et suivant les instructions du client (voir Chapitre 2.3).

(2) Le contractant se conformera toujours aux instructions correspondantes du client, même au-delà de la fin de ce contrat.

(3) Si une suppression conforme à la protection des données ou une restriction correspondante du traitement des données n'est pas possible, le contractant se charge de la destruction des supports de données dans le respect de la protection des données et autres matériels sur la base d'une commande individuelle du client, ou restitue ces supports de données au client, sauf si cela a déjà été convenu dans le contrat. Dans des cas particuliers déterminés par le client, le stockage ou la remise a lieu. L'indemnisation et les mesures de protection doivent être convenues séparément, à moins qu'elles n'aient déjà été convenues dans le contrat.

(4) Des copies ou des duplicatas ne sont pas créés sans la connaissance du client. Les exceptions sont les duplications temporairement nécessaires sur le plan technique, dans la mesure où une altération du niveau de protection des données convenu ici est exclue.

(5) Les supports de données dédiés provenant du client ou utilisés pour le client sont spécialement marqués et sont soumis à une gestion continue. Ils doivent être stockés de manière adéquate en tout temps et ne doivent pas être accessibles à des personnes non autorisées. Les entrées et sorties sont documentées.

(6) À la fin de la relation contractuelle ou à tout moment à la demande du client, le contractant doit soit détruire les données traitées dans le cadre de la commande, les supports de données et tous les autres matériaux selon le choix du client, soit les remettre au client. Toutes les copies existantes des données doivent également être détruites. La destruction doit être effectuée de manière à ce qu'une restauration même des informations résiduelles avec un effort raisonnable ne soit plus possible.

(7) Le contractant est obligé d'assurer la restitution ou la suppression immédiate également chez les sous-traitants.

(8) Le contractant doit fournir la preuve de la destruction appropriée et la présenter immédiatement au client.

(9) Les documentations servant de preuve d'un traitement approprié des données doivent être conservées par le contractant conformément aux délais de conservation respectifs même au-delà de la fin du contrat. Il peut les remettre au client à la fin du contrat pour son déchargement.

Remarque : cette traduction n’est fournie qu’à des fins de commodité. La version allemande de ce document est la version juridiquement contraignante puisque l'entreprise est basée en Allemagne.

MESURES TECHNIQUES ET ORGANISATIONNELLES (MTO) POUR LA PROTECTION DES DONNÉES

PSEUDONYMISATION (ART. 32 (1) AL. A RGPD ; ART. 25 (1) RGPD)
Traitement des données à caractère personnel de manière à ce que les données ne puissent plus être attribuées à une personne concernée spécifique sans recourir à des informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles.

1. PSEUDONYMISATION / MESURES TECHNIQUES-ORGANISATIONNELLES – PROJET SPÉCIFIQUE

Détails/Remarques :
Les données de cookies ne peuvent pas être attribuées à une personne spécifique. La pseudonymisation des données est effectuée via les sous-prestataires de services. Ainsi, les sous-prestataires de services garantissent que les cookies ne peuvent pas être attribués à une personne spécifique.

2. CONFIDENTIALITÉ (ART. 32 (1) AL. B RGPD)

La capacité d'assurer la confidentialité des systèmes et services relatifs au traitement de manière permanente.

2.1 Contrôle d'accès – Empêcher l'accès non autorisé aux installations de traitement des données, par exemple :

- Mesures aptes à empêcher l'accès des personnes non autorisées aux installations de traitement des données où sont traitées ou utilisées des données à caractère personnel.

- Contrôle d'accès

- Clés de sécurité magnétiques personnalisées : Chaque employé reçoit une clé de sécurité magnétique personnelle qui contrôle l'accès à nos locaux. Cette clé est unique et attribuée individuellement pour garantir que seules les personnes autorisées ont accès aux zones sensibles. La perte ou la cession de clés de sécurité à des tiers doit être signalée immédiatement, et des mesures appropriées (désactivation de la clé) sont prises pour maintenir la sécurité.

2.2 Contrôle d'accès – Aucune utilisation non autorisée du système, par exemple :

- Mesures aptes à empêcher que les systèmes de traitement des données puissent être utilisés par des personnes non autorisées.

- Contrôle d'accès / Systèmes techniques – Mesures de base

- L'accès aux systèmes informatiques est possible uniquement avec un mot de passe.
- Les mécanismes de verrouillage automatique des systèmes informatiques sont activés via Microsoft Cloud 365.
- Les mises à jour du système sont effectuées automatiquement.
- Tous les systèmes informatiques sont équipés d'un logiciel antivirus / pare-feu.
- Les clients attribuent eux-mêmes les mots de passe, qui peuvent être changés après la première mise en service et ne sont pas connus du prestataire.
- Un rappel automatique que les mots de passe doivent être changés par l'utilisateur tous les 91 jours.

2.3 Contrôle d'accès

- Mesures garantissant que les personnes autorisées à utiliser un système de traitement des données peuvent accéder uniquement aux données auxquelles leur autorisation d'accès s'applique, et que les données à caractère personnel ne peuvent pas être lues, copiées, modifiées ou supprimées sans autorisation lors du traitement, de l'utilisation et après le stockage.

- Mise en place d'un concept d'autorisation, où l'accès au propre espace de connexion et aux données de campagne est attribué exclusivement à chaque client ;
- Enregistrement des modifications dans les fichiers journaux ;
- Seul le personnel fonctionnel a accès à toutes les données des clients et des campagnes.
- Les employés ont des droits d'accès individuels selon leurs besoins.
- Contrôle de séparation assurant que les données des clients sont stockées séparément de manière logique des autres données.

3. INTÉGRITÉ (ART. 32 (1) AL. B RGPD)

La capacité d'assurer l'intégrité des systèmes et services relatifs au traitement de manière permanente (protection contre la modification ou la suppression non autorisées lors du stockage électronique, de la transmission ou du transport), par exemple :

- Les données peuvent être saisies et traitées par le client et, selon la commande, également par le prestataire.
- L'accès par le client est enregistré.
- Comptes de courrier électronique chiffrés.

4. DISPONIBILITÉ ET RÉSILIENCE (ART. 32 (1) AL. B RGPD)

La capacité d'assurer la disponibilité et la résilience des systèmes et services relatifs au traitement de manière permanente (protection contre la destruction ou la perte accidentelle ou intentionnelle), par exemple :

- Les données de campagne sont également sécurisées par nos sous-prestataires de services.

5. RÉTABLISSEMENT RAPIDE (ART. 32 (1) AL. C RGPD)

La capacité de rétablir rapidement la disponibilité des données à caractère personnel et l'accès à celles-ci en cas d'incident physique ou technique, par exemple :

- En cas de perte de données ou si une perte est identifiée, la direction est informée. Pour les données de campagne, le sous-prestataire de services est informé, qui restaure les données via les systèmes de sauvegarde.

6. PROCÉDURES D'EXAMEN RÉGULIER, D'ÉVALUATION ET D'ÉVALUATION (ART. 32 (1) AL. D RGPD ; ART. 25 (1) RGPD)

Une procédure pour l'examen régulier, l'évaluation et l'évaluation de l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement doit être en place, par exemple :

- Les employés de MINT Square sont régulièrement formés en matière de droit de la protection des données et sont familiarisés avec les instructions procédurales et les directives d'utilisation pour le traitement des données en nom, y compris en ce qui concerne le droit d'instruction du client.
- Chaque employé est obligé de respecter les exigences de protection des données conformément au RGPD au plus tard le premier jour de son activité.
- Il existe un registre de traitement au sens de l'Art. 30 (1), (2) RGPD et un processus pour l'évaluation d'impact (DSFA), qui est réalisé régulièrement.

7. PRÉRÉGLAGES FAVORABLES À LA PROTECTION DES DONNÉES (ART. 25 (2) RGPD)

Le responsable du traitement prend des mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel nécessaires à chaque finalité spécifique du traitement sont traitées.

- Des informations sur les cookies sont collectées
- MINT Square utilise des cookies de navigateur via le sous-prestataire de services pour stocker des informations sur les préférences des visiteurs du site web, telles que l'opt-out et l'ID de navigateur unique du visiteur, et pour stocker des informations sur la fonctionnalité du serveur d'annonces du sous-prestataire de services – capping de fréquence, rotation des annonces, attribution des médias après un clic.
- Le sous-prestataire de services lit les cookies de navigateur à chaque requête HTTP-GET au serveur et transmet soit l'ID de navigateur du visiteur, soit des informations indiquant que les cookies sont désactivés ou que le visiteur a été exclu du service par le prestataire à chaque transaction – impression, clic, visite de site web, autre événement.
- Les sous-prestataires de services ne placent des cookies sur le navigateur du visiteur que lorsque cela est justifié – certaines fonctions du serveur d'annonces ont été utilisées ou pour prolonger la durée de vie des cookies.
- Les sous-prestataires de services n'utilisent pas d'autres cookies (par exemple, cookies Flash) ou des fonctions similaires pour suivre le visiteur ou le navigateur du visiteur. Les sous-prestataires de services ne stockent aucune information privée ou sensible dans les cookies de navigateur.