Politique

Traitement des données au sein de G4S France

Securing Your World

Table des matières

1. Introduction

Le 14 avril 2016, le Parlement européen a adopté le règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel concernant la libre circulation de ces données et abrogeant la directive 95/46/EG. Cette réglementation est mieux connue sous le nom de *General Data Protection Regulation* (GDPR)[1].

Ce document est basé sur le GDPR et reflète les principes généraux de la politique de confidentialité de G4S France[2]. En matière de confidentialité, il est fait référence à la protection des données personnelles. Le traitement des données personnelles est nécessaire pour les processus d'affaires au sein de G4S ainsi que pour les processus que G4S a sous-traités à des tiers. Cela doit être fait dans un certain but, subsidiaire, proportionné et prudent, car une mauvaise manipulation des données personnelles peut entraîner des dommages importants pour les clients, les fournisseurs, les employés, les autres parties concernées et G4S elle-même. G4S attache une grande importance à la protection la plus précise des données personnelles qui lui sont fournies et à la façon dont ces données sont traitées. La responsabilité de la protection des données personnelles incombe à la direction de G4S.

En décrivant les mesures contenues dans ce document de politique, G4S prend la responsabilité d'optimiser la qualité de la sécurité des données personnelles.

1.1 Données personnelles, data et information

La protection des données personnelles (vie privée), des datas et des informations sont interdépendantes, mais il existe une distinction entre les termes. La vie privée est le droit de maîtriser vos propres données personnelles. Les datas sont une quantité de données. L'information est considérée comme des données ayant une certaine signification. En bref, les datas sont nécessaires pour obtenir des informations et les datas doivent être protégées afin que les données personnelles des personnes concernées, et donc leur vie privée, ne soient pas, ou le moins possible, violées.

1.2 Portée et objectifs de la politique

Cette politique concerne le traitement des données personnelles sous la responsabilité de G4S. Il concerne à la fois les processus d'entreprise internes et les processus externalisés à des tiers. G4S doit collecter et utiliser certaines informations sur les individus à des fins commerciales. Ceux-ci peuvent être des clients, des fournisseurs, des contacts d'affaires, des employés ou d'autres personnes.

[1] Dans ce document, le terme GDPR est utilisé.
[2] Ci-après nommée G4S. Ce document de politique est applicable à G4S SECURE SOLUTIONS FRANCE et ses sociétés liées

La politique est d'application au traitement entièrement ou partiellement automatisé / systématique des données personnelles ainsi qu'au traitement non automatisé des données personnelles qui se déroule sous la responsabilité de G4S.

G4S interprète largement la protection des données personnelles. Il existe une relation et un chevauchement partiel avec la sécurité de l'information. La sécurité de l'information est le nom collectif des processus qui visent à garantir la fiabilité de toutes les formes d'informations au sein d'une organisation. La fiabilité est déterminée en surveillant :

- Disponibilité: assurer la disponibilité de l'information et de l'équipement de traitement de l'information au bon endroit et au bon moment pour les utilisateurs.
- Intégrité: assurer l'exactitude, l'exhaustivité, la rapidité et le caractère vérifiable de l'information et de son traitement.
- Confidentialité: protéger les informations contre tout traitement non autorisé.

La sécurité de l'information vise à garantir la continuité de l'information et à limiter les conséquences des incidents de sécurité à un niveau acceptable prédéterminé, mais aussi à optimiser la qualité du traitement et la sécurité des données personnelles, à quoi un équilibre sain et bon doit être trouvé entre sécurité, confidentialité et fonctionnalité.

G4S respecte la vie privée des personnes impliquées. Les données personnelles doivent être protégées de manière adéquate contre les infractions, qu'elles soient illégales ou non. Cela implique que G4S doit se conformer aux lois et règlements pertinents relatifs au traitement des données personnelles.

Les objectifs de cette politique sont les suivants:

- Établir des normes : la base de la sécurité des données personnelles est le Group Information Security Mandatory Minimal Security Controls (MMSC)[3] Implementation Standard de G4S et les meilleures pratiques de l'industrie de la sécurité.
- Fournir un cadre : la politique fournit un cadre pour tester le traitement (y compris futur) des données personnelles à une norme ou un « best practice » convenu.
- Investir des tâches, des pouvoirs et des responsabilités dans l'organisation.
- Prendre des responsabilités: la direction doit définir les points de départ et l'organisation du traitement des données personnelles pour l'ensemble de G4S et doit les propager.
- En tant que leader du marché, être un exemple pour d'autres organisations de sécurité.
- Mise en œuvre de la politique en faisant des choix clairs dans les mesures et en appliquant un contrôle actif à la mise en œuvre des mesures politiques.
- Sensibiliser les employés (externes) de G4S à l'importance et à la nécessité de protéger les données personnelles.
- Etre conforme à la législation française et européenne.

[3] Le MMSC est la norme de sécurité de l'information utilisée par G4S et est un dérivé de la norme ISO 27001; la norme internationale pour la sécurité de l'information

1.3 Définitions

Tous les termes spécifiques utilisés dans ce document ont la signification qu'ils ont reçue dans le GDPR. Les termes qui ne sont pas définis dans le GDPR ont leur signification linguistique générale. Les termes suivants ont la signification suivante :

- Privacy by default: mettre les paramètres d'un produit ou d'un service par défaut au paramètre le plus respectueux de la vie privée.
- Privacy by design: attention à la vie privée tout au long du cycle de vie d'un système, de la conception à l'enlèvement du système.

1.4 Structure du document

Les sujets suivants sont abordés tour à tour: principes du traitement des données personnelles, organisation du traitement des données personnelles, mise en œuvre de la politique, traitement adéquat et soigné des données personnelles, incidents, droits de la personne concernée et gestion du document.

2. Les principes de traitement des données personnelles

Le point de départ de la politique est que les données personnelles sont traitées avec soin et en conformité avec les lois et règlements en vigueur. Un bon équilibre doit être trouvé entre l'importance pour G4S de traiter les données personnelles et l'intérêt de la personne concernée à faire ses propres choix en ce qui concerne ses données.

Les principes suivants ont été élaborés pour répondre au point de départ:

- Chaque traitement de données personnelles est basé sur l'une des bases légales mentionnées dans le GDPR.
- Les données personnelles ne sont traitées qu'à des fins clairement définies et justifiées. Ces objectifs ont été formulés spécifiquement et avant le traitement.
- Lors du traitement des données personnelles, la quantité et le type de données sont limités aux données personnelles nécessaires à l'utilisation spécifique. Les données doivent être adéquates, pertinentes et non excessives compte tenu de cet objectif.
- Le traitement des données personnelles s'effectue de la manière la moins radicale et doit être proportionné au but recherché.
- Des mesures sont prises pour assurer autant que possible que les données personnelles à traiter sont correctes et à jour.
- Les données personnelles sont correctement sécurisées selon les normes de sécurité applicables.
- Les données personnelles ne sont pas traitées plus longtemps que nécessaire aux fins du traitement, les périodes de stockage et de destruction applicables sont respectées.
- Un registre des activités de traitement est établi.
- Privacy by design et privacy by default sont utilisées.
- Toute personne concernée a le droit de rectifier, de modifier les données, de limiter le traitement et à la transférabilité, comme indiqué au chapitre 7 de la présente politique.

3. Organisation en ce qui concerne le traitement des données personnelles

G4S France dispose d'une équipe de projet GDPR dirigée par le chef de projet (Manager Public & Legal Affairs). G4S nommera un Data Protection Officer (également appelé Data Officer ou Privacy Officer) au plus tard le 25 mai 2018. Jusque-là, les tâches et responsabilités du Data Protection Officer relèvent de l'autorité du chef de projet. Toutes les Business Units (BU) de G4S France sont représentées dans l'équipe de projet GDPR.

4. Implémentation de la politique

La direction de G4S à la responsabilité finale du traitement des données personnelles. Cependant, le traitement réel est effectué au sein de différentes entités de G4S. Ce chapitre décrit comment la politique est mise en œuvre.

4.1 Plan, Do, Check, Act-cyclus

La protection de la vie privée est un processus continu de qualité. Plan, Do, Check, Act (PDCA) forment ensemble le système de gestion de la vie privée. Ce cycle de qualité est illustré à la figure 1.

Figure 1 PDCA-cyclus

Explication du PDCA-cyclus:

- Plan : Le cycle commence par l'élaboration d'une politique. Cette politique est basée sur la législation et la réglementation, les normes du secteur. En outre, des lignes directrices et des normes sont élaborées. La politique est révisée chaque année et, si nécessaire, ajustée dans l'intervalle.
- Do : La politique constitue la base pour créer des actions de sensibilisation, effectuer des mesures dans l'organisation et prendre des dispositions. La mise en œuvre de ces actions fait partie du processus de travail quotidien. La politique est traduite en plans concrets.

- Check : Le contrôle de la conformité à la politique est effectué en faisant des audits au sein de l'organisation et en menant des consultations périodiques avec des intervenants internes. Le but du contrôle est de sécuriser la protection des données personnelles et de se conformer aux lois et règlements. Les résultats des audits sont communiqués aux départements / BU concernés et, si nécessaire, à la direction. En outre, des rapports de gestion périodiques sont rédigés.
- Act : Sur base des audits et des consultations, les processus sont évalués et des propositions d'amélioration sont faites et les meilleures pratiques développées. S'il y a des propositions d'amélioration drastiques, cette décision sera soumise à la direction comme une décision.

4.2 Répartition des responsabilités

Le traitement des données personnelles doit être considéré comme une responsabilité déléguée de la direction aux différentes BU. Les managers et les directeurs sont principalement responsables du traitement soigneux des données personnelles dans leurs processus d'entreprise. Cela inclut également l'introduction des mesures, la mise en œuvre et l'exécution de celles-ci. De plus, il incombe aux managers et aux directeurs de discuter de cette politique avec toutes les parties concernées.

La manipulation prudente des données personnelles est une responsabilité de chaque employé de G4S. Le traitement soigneux des données personnelles comprend:

- Le principe d'un bureau propre / écran propre ;
- Ne pas laisser les marchandises de l'entreprise avec des données dans la voiture ;
- Utiliser le bac à papier et le vider dans le container à papier sécurisé ; ou broyer les documents papier
- Signaler au superviseur, de manière proactive, les risques liés à la vie privée;
- Etc.

Les employés doivent se comporter avec intégrité concernant le traitement des données personnelles. Il est inacceptable que, par un comportement intentionnel ou non intentionnel, surviennent des situations qui peuvent entraîner des dommages ou la perte de la réputation de G4S ou des personnes impliquées. Pour cette raison, des codes de conduite ont été élaborés et mis en œuvre et une attention constante est portée à la sensibilisation.

5. Traitement approprié et soigné des données personnelles

5.1 Traitements

Le traitement des données personnelles doit être basé sur l'un des motifs légaux décrits dans le GDPR. Les motifs légaux sont les suivants:

a) La personne concernée a donné son autorisation pour le traitement de ses données personnelles dans un ou plusieurs buts spécifiques;
b) Le traitement est nécessaire à l'exécution d'une convention à laquelle l'intéressé est partie, ou à prendre des mesures à la demande de l'intéressé pour la conclusion d'une convention;
c) Le traitement est nécessaire pour se conformer à une obligation légale qui incombe au responsable du traitement;
d) Le traitement est nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique;
e) Le traitement est nécessaire pour l'accomplissement d'une tâche d'intérêt général ou d'une tâche dans l'exercice de l'autorité publique confiée au responsable du traitement;
f) Le traitement est nécessaire à la défense des intérêts légitimes du responsable du traitement ou d'un tiers, sauf si les intérêts ou les droits fondamentaux et libertés fondamentales de la personne concernée qui exigent la protection des données à caractère personnel l'emportent sur ces intérêts, notamment si la personne est un enfant.
g) Toute future extension possible des motifs légaux déterminés dans le GDPR.

La personne responsable du processus d'entreprise décrit les objectifs du traitement à l'avance. Chaque traitement est signalé au privacy officer. Le privacy officer vérifie ensuite si le traitement est nécessaire et si les fins sont juridiquement valides. Le privacy officer tient un registre des activités de traitement conformément au GDPR.

Les systèmes dans lesquels les données personnelles sont traitées doivent être conformes aux exigences de Mandatory Minimum Security Controls (MMSC). Dans le cas des changements d'infrastructure ou de l'achat de nouveaux systèmes, un Privacy Impact Assessment (PIA) est effectué à l'avance (voir plus loin). De plus, les principes du privacy by design et privacy by default, tels que décrits dans le GDPR, sont utilisés.

Les données personnelles sensibles[4] ne seront pas traitées, sauf si cela est nécessaire pour l'exécution d'une tâche statutaire ou d'un règlement. Si des données personnelles sensibles sont traitées, elles sont séparées et sont plus sécurisées que d'autres données personnelles.

[4] Les données personnelles spéciales sont conformes à l'article 9 GDPR: origine raciale ou ethnique, opinions politiques, croyances religieuses ou philosophiques, appartenance à un syndicat, données génétiques et biométriques, données sur la santé, comportement sexuel / données sur l'orientation sexuelle et toutes les futures extensions possibles de ce concept.

5.2 Protection des données

G4S prendra les mesures organisationnelles et techniques appropriées pour protéger et promouvoir la disponibilité, l'intégrité et la confidentialité des données personnelles et pour prévenir la perte, la contrefaçon et le traitement illégal de données personnelles. Outre la gestion de la norme MMSC, il existe plusieurs manières de sécuriser la protection des données, telles que l'exécution d'un PIA, la classification des données et la consignation de l'utilisation des données.

5.2.1. Privacy Impact Assessment (PIA)

L'exécution d'un PIA est un moyen de sécuriser la protection des données. Un PIA reflète les risques pour la vie privée des traitements existants et nouveaux de données. Des mesures peuvent être prises sur cette base. Conformément au GDPR, un PIA doit être réalisé dans les situations suivantes:[5]

- S'il est question d'une évaluation des aspects personnels systématiques et étendus, y compris le profilage;
- Les données personnelles spéciales sont traitées à grande échelle;
- Lorsque les personnes sont suivies à grande échelle et systématiquement dans une zone accessible au public (par exemple avec la surveillance par caméra).

5.2.2. Classification de data

Chaque système dans lequel les données personnelles sont traitées est différent et doit être classé sur mesure. La classification des données vise à déterminer la disponibilité, l'intégrité et la confidentialité du système. Cela indique clairement quelles mesures sont nécessaires pour protéger le système en question.

5.2.3. Logging de l'utilisation des données

Chaque système automatisé qui traite des données personnelles doit conserver la journalisation des opérations de traitement. Au minimum les éléments suivants doivent être enregistrés: quel utilisateur, quelle heure et ce qui est en cours de traitement.

5.2.4. Périodes de conservation

Les données personnelles ne peuvent pas être conservées plus longtemps que nécessaire aux fins pour lesquelles elles ont été utilisées ou collectées. Les périodes de conservation peuvent être déterminées légalement ou par G4S. Les données personnelles doivent être détruites dès que la période de conservation a expiré.

[5] En temps voulu, l'Autorité de surveillance publiera une liste des opérations de traitement pour lesquelles un PIA est obligatoire. Cette liste n'est pas encore connue lors de la rédaction de ce document, mais elle lui est pleinement applicable.

Si les données personnelles sont destinées à des fins historiques, statistiques ou scientifiques, ces données doivent être conservées dans des archives séparées et être également désignées de cette manière.

5.3 Contrats de traitement des données à caractère personnel

G4S externalise les processus et les services à des tiers. L'externalisation des processus et des services comporte des risques en matière de traitement des données et de sécurité de l'information. G4S reste responsable du traitement de ces données. Afin de pouvoir gérer la responsabilité, un contrat de traitement des données à caractère personnel est conclu pour chaque externalisation où des données personnelles sont impliquées.

Le privacy officer est le propriétaire du contrat et l'ajuste si besoin. Il est de la responsabilité du manager du département ou du directeur d'une BU de conclure et de gérer ces contrats. Le privacy officer vérifie si cela est respecté et donne des conseils.

6. Incidents

6.1 Incidents de sécurité et violations de données

Des incidents peuvent survenir et il faut réagir de manière adéquate. Il peut s'agir d'un incident de sécurité ou d'une violation de données. Un incident de sécurité est un événement qui peut affecter l'intégrité, la confidentialité ou la disponibilité des données.[6] Une violation de données est l'accès ou la destruction, la modification ou la divulgation de données personnelles dans une organisation sans que cela ne soit intentionnel de la part de cette organisation, illégale ou non.[7] Avec une violation de données, il est certain que des données personnelles ont été perdues ou qu'un traitement illégal ne peut être exclu.[8]

6.2 Notification et enregistrement

Les incidents de sécurité et les violations de données doivent être signalés via privacy.gdpr@fr.g4s.com. Chaque incident est enregistré. La période de conservation d'un incident est de trois ans.

L'adresse mail est destinée aux employés internes et aux parties prenantes externes.

Conformément au GDPR, G4S doit faire rapport à l'Autorité de surveillance (AS) dans un délai de 72 heures en cas de violation de données. Le rapport à l'AS peut et ne peut être fait que par le privacy officer.

Conformément au GDPR, G4S doit informer les parties concernées de la violation de données. Cela doit être fait si la violation de données a des conséquences défavorables pour la vie privée de la personne concernée.[9]

Tous les deux mois, le privacy officer fournit un update des incidents qui se sont produits à la direction. De plus, le privacy officer établit un rapport annuel.

6.3 Equipe Privacy

Le privacy officer évalue l'incident et détermine en premier lieu s'il s'agit d'un incident de sécurité ou d'une violation de données et si les personnes concernées doivent être informées. L'évaluation est ensuite partagée avec l'équipe Privacy pour déterminer le jugement final. En plus du Privacy Officer, l'équipe Privacy comprend au moins le manager Legal & Public Affairs

[6] Un exemple d'incident de sécurité est le vol d'un laptop.
[7] Un exemple de violation de données est le vol d'un laptop contenant des données clients financières non cryptées.
[8] Une violation de données est toujours un incident de sécurité. Un incident de sécurité n'est pas toujours une violation de données.
[9] Un exemple de situation où la personne concernée doit être mise au courant est la situation où des mots de passe et noms de code sont violés.

et le Managing Director. La décision de signaler ou non un incident à l'AS se fait toujours en consultation avec la direction.

Pour chaque incident, l'équipe Privacy est complétée par le manager/directeur du processus d'affaires impliqué et un membre du département IT. L'équipe Privacy anticipe une réaction possible dans les médias.

7. Droits des personnes concernées

7.1 Communication transparente

Pour G4S, il est important que les employés, les clients, les fournisseurs et les autres parties prenantes puissent avoir l'assurance que leurs données personnelles sont traitées de manière sécurisée et avec soin. Cette confiance est créée en fournissant un aperçu de la façon dont les données sont traitées et gérées, c'est-à-dire :

- Quelles données sont collectées;
- Dans quel but ces données sont-elles recueillies;
- Que se passe-t-il ensuite avec ces données;
- Qui a accès aux données;
- Quels droits ont les personnes concernées.

L'information est fournie de telle sorte que la personne concernée comprenne son contenu.

7.2 Droit d'accès aux données personnelles

Conformément au GDPR, toute personne concernée a le droit de demander lesquelles de ces données personnelles sont traitées et à quelles fins. Une demande d'inspection des mineurs n'ayant pas encore atteint l'âge de 16 ans est faite par leur représentant légal.

7.3 Droit à la rectification des données personnelles

Conformément au GDPR, la personne concernée a le droit de faire corriger, modifier ou compléter immédiatement ses données personnelles, si celles-ci sont factuellement incorrectes, incomplètes ou non pertinentes.

7.4 Droit au changement de données

Conformément au GDPR, la personne concernée a le droit d'obtenir le changement sans délai des données personnelles le concernant si l'une des conditions suivantes est remplie:

- Les données personnelles ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées ou traitées;
- La personne concernée retire le consentement sur lequel repose le traitement conformément à l'article 6, paragraphe 1, point a) du GDPR, ou à l'article 9, paragraphe 2, point a) du GDPR et il n'existe aucune autre base juridique pour le traitement;
- La personne concernée s'oppose au traitement conformément à l'article 21, paragraphe 1 du GDPR, et il n'existe pas de motifs justifiés faisant autorité pour le traitement, ou la personne concernée s'oppose au traitement conformément à l'article 21, paragraphe 2 du GDPR;
- Les données personnelles ont été traitées illégalement;

- Les données personnelles doivent être supprimées afin de se conformer à une obligation légale prévue par la législation de l'Union européenne ou des États membres qui incombe au responsable du traitement;
- Les données personnelles ont été collectées dans le cadre d'une offre de services de la société d'information telle que visée dans le GDPR.

7.5 Droit à la restriction du traitement

Conformément au GDPR, toute personne concernée a le droit d'obtenir la limitation du traitement auprès de G4S si l'une des conditions suivantes s'applique:

- L'exactitude des données personnelles est contestée par la personne concernée pendant une période permettant au responsable du traitement de vérifier l'exactitude des données personnelles;
- Le traitement est illégal et la personne concernée s'oppose à l'effacement des données personnelles et demande à la place de limiter leur utilisation;
- Le responsable du traitement n'a plus besoin des données personnelles à des fins de traitement, mais la personne concernée en a besoin pour l'établissement, l'exercice ou la justification d'une réclamation légale;
- La personne concernée s'est opposée au traitement conformément à l'article 21, paragraphe 1 du GDPR, en attendant la réponse à la question de savoir si les motifs justifiés du responsable du traitement sont supérieurs à ceux de la personne concernée.

7.6 Droit à la portabilité des données

Conformément au GDPR, la personne concernée a le droit d'obtenir les données personnelles la concernant, qu'elle a fournies à un responsable du traitement, sous une forme structurée, actuelle et lisible, et a le droit de transférer ces données à un autre responsable sans avoir à être gênée par le responsable du traitement auquel les données personnelles avaient été fournies, si:

- Le traitement est basé sur une autorisation en vertu de l'article 6, paragraphe 1, point a) du GDPR, ou de l'article 9, paragraphe 2, point a) du GDPR, ou sur un accord en vertu de l'article 6, paragraphe 1, point b) du GDPR;
- et le traitement est effectué par des processus automatisés.

7.7 Introduction de la demande

Les demandes d'inspection, de rectification, de modification de données, de limitation ou de transfert peuvent être adressées par écrit à Koning Boudewijnlaan 30, 1800 Vilvoorde, Belgique, à l'attention du Data Protection Officer ou par mail à privacy.gdpr@fr.g4s.com avec copie au responsable de traitement de G4S Secure Solutions France.

G4S répondra à la demande par écrit dans un délai de quatre semaines au plus tard. G4S demande par la présente une détermination correcte de l'identité de la personne qui soumet la demande. Dès que la demande est justifiée, G4S prend immédiatement les mesures nécessaires pour se conformer à la demande.

En cas de décision sur une demande, la personne concernée peut présenter une objection écrite si elle est d'avis que les dispositions légales concernant la protection des données personnelles n'ont pas été correctement appliquées. Si la personne concernée n'est pas d'accord avec la réponse de G4S, la personne concernée a la possibilité de poursuivre son action en justice.

8. En conclusion

Cette politique a été déterminée par la direction de G4S France en date du 25 mai 2018. Le Délégation Unique du Personnel a été informé de ce document de politique.

Les changements à cette politique sont annoncés via le site Web de G4S et la version la plus récente est publiée sur http://www.g4s.fr/fr-fr/privacy.

Pour toute question et/ou commentaire concernant cette politique, veuillez contacter le privacy officer.