

ANNEXE I.

NORMES DE PROTECTION DES DONNEES POUR LE DEVELOPPEMENT D'OUTILS NUMERIQUES DESTINES AUX PARTENAIRES DE LA GIZ

Les données à caractère personnel sont toutes les informations qui, seules ou en combinaison avec d'autres informations, peuvent conduire à l'identification d'une personne physique ou être attribuées à cette personne. Cela va des identifiants directs tels que les noms, les adresses e-mail, aux identifiants indirects ou distants tels que la taille exacte de la ferme ou simplement l'heure exacte d'une visite sur le site Web.

Le développement d'un système de traitement de données n'implique pas nécessairement le traitement de données à caractère personnel. Cependant, étant donné que ces systèmes, tels que les applications, les sites Web, les plates-formes Internet, les logiciels, les caméras, etc., sont destinés au traitement des données à caractère personnel, certaines conditions préalables doivent être remplies. Les systèmes doivent satisfaire à l'exigence de nécessité et tenir compte des obligations en matière de protection des données dès la conception et protection des données par défaut. Le présent document offre des conseils pratiques sur la conformité à ces exigences.

1. L'EXIGENCE DE NÉCESSITÉ

Un outil de traitement des données doit être conçu pour traiter des données à caractère personnel uniquement lorsque leur objectif ne peut être atteint sans ces données. Par exemple, si des informations anonymes servent à cette fin, aucune donnée personnelle ne doit être traitée. Voici des exemples d'informations anonymes :

- tranche d'âge au lieu de l'âge exact ou de la date de naissance (1-5 ans; 6-10 ans; 11-15 ans, etc.);
- fourchette de revenu au lieu de son revenu exact (1000-3000 EUR; 4000-6000 EUR; 7000-10000 EUR etc.) ;
- la taille de la ferme varie (1 à 3 acres; 4 à 6 acres; 7 à 10 acres; plus de 10 acres);
- Fourchette du nombre de personnes vivant dans un ménage (1 à 3 personnes; 4 à 6 personnes; 7 à 10 personnes, etc.);
- préférez des termes généraux à des termes spécifiques (par exemple, pour déterminer son statut d'emploi, vous pouvez indiquer: employé, travailleur indépendant et chômeur, au lieu d'une profession particulière);

- utilisez des groupements géographiques plus importants au lieu de groupements plus petits (par exemple, identifier une région ou un département au lieu d'un village ou quartier).

De plus, les questions devraient exiger des réponses « oui » ou « non », et lorsque des renseignements précis sont requis, des options peuvent être énumérées pour que la personne choisisse. Lorsque la réponse de la personne ne fait pas partie des réponses suggérées, elle devrait être tenue de choisir « autre », sans laisser de place à la personne pour divulguer des renseignements détaillés qui pourraient l'identifier de façon unique.

Tout autre identifiant (figures/lieux/etc.) doit être dilué pour rendre l'identification impossible.

Cette catégorie d'informations est considérée comme anonyme car elle ne peut pas conduire à l'identification d'une personne physique, ni être attribuée à cette personne. Dans le cas où des données personnelles telles que (mais sans s'y limiter) des noms, des adresses IP, des adresses e-mail, etc. doivent être traitées, l'outil doit respecter les exigences suivantes en matière de protection des données dès la conception et protection des données par défaut énoncées aux paragraphes 2 et 3 ci-dessous.

2. PROTECTION DES DONNÉES DÈS LA CONCEPTION ET PAR DÉFAUT

Le système devrait être conçu de manière à tenir compte des principes de protection des données (en particulier la licéité, la minimisation des données, la transparence, l'intégrité et la confidentialité, l'exactitude, la limitation de la conservation et la responsabilité), ainsi que des nombreux droits de la personne concernée, comme expliqué au paragraphe 3 ci-dessous. En outre, il faut s'assurer que:

- par défaut, les fonctions de confidentialité du système sont activées et les utilisateurs ne doivent prendre aucune mesure pour protéger leurs données personnelles;
- des caractéristiques de confidentialité sont intégrées dans la conception du système pour s'assurer que le système ne peut jamais fonctionner sans ces fonctionnalités;
- la protection tout au long du cycle de vie est prise en compte.

3. PRINCIPES DE PROTECTION DES DONNÉES ET DROITS NÉCESSAIRES

a. Licéité du traitement des données

En vertu de ce principe, les données à caractère personnel ne doivent être traitées que si le responsable du traitement est autorisé par la loi à le faire, et l'un des moyens généralement autorisés est de traiter ces données avec le consentement de la personne concernée. Le consentement est l'une des bases juridiques les plus appropriées pour le traitement des données à caractère personnel avec des outils numériques. Toutefois, pour qu'un tel consentement soit valide, il doit remplir les conditions suivantes :

- par défaut, toutes les fonctionnalités nécessitant un consentement doivent être désactivées, sauf si l'utilisateur les active ;
- le consentement doit être donné dans un but spécifique (et non pour un ensemble de finalités) et lorsque le consentement est requis pour plus d'une finalité, il doit être demandé séparément pour chacune d'elles, par exemple deux cases à cocher distinctes sont respectivement requises pour l'utilisation de cookies non essentiels et le partage de données personnelles avec un tiers;
- la personne concernée doit être bien informée de l'activité de traitement, y compris de son droit de retirer son consentement (voir l'alinéa e. « Transparence » ci-dessous);
- le consentement doit être sans ambiguïté (par le biais d'une action positive, par exemple en cochant une case, mais pas en désactivant une case pré-cochée. Le silence ne serait pas considéré comme une acceptation);
- chaque fois que des catégories particulières de données à caractère personnel (telles que des données biométriques, des données relatives à la santé, à l'orientation sexuelle ou à la vie sexuelle, aux convictions religieuses ou philosophiques, etc.) sont traitées, le consentement doit être explicite. Cela s'applique également au profilage et à la prise de décision automatisée. C'est-à-dire que le système doit exiger une authentification (par exemple par SMS) ou une signature électronique, pour écarter tout doute quant à savoir si le consentement a été donné ou non. Le consentement explicite est également requis pour accéder à son compte bancaire ou traiter des informations financières lors de paiements en ligne;

- le consentement doit être facilement révoable et le refus de consentir ne doit pas entraîner le refus de service ou être préjudiciable de quelque manière que ce soit à l'utilisateur, sinon un tel consentement ne serait pas considéré comme ayant été donné librement. Par exemple, la personne concernée devrait être capable de refuser de consentir à l'utilisation de cookies non essentiels tout en ayant accès au site Web. Si le consentement est une condition préalable à l'accès au site Web, ce consentement serait invalide.

i. Cookies essentiels (non soumis à consentement)

Selon le WP29 (aujourd'hui Comité européen de la protection des données), les cookies suivants, considérés comme essentiels, peuvent être utilisés sans le consentement de la personne concernée sous certaines conditions, s'ils ne sont pas utilisés à d'autres fins:

- les cookies d'entrée utilisateur (session-id), pour la durée d'une session ou les cookies persistants limités à quelques heures dans certains cas;
- les cookies d'authentification, utilisés pour les services authentifiés, pour la durée d'une session ;
- les cookies de sécurité centrés sur l'utilisateur, utilisés pour détecter les abus d'authentification, pour une durée persistante limitée (quelques heures);
- les cookies de session de lecteur de contenu multimédia, tels que les cookies Flash Player, pour la durée d'une session;
- les cookies de session d'équilibrage de charge, pour la durée de la session;
- cookies persistants de personnalisation de l'interface utilisateur, pour la durée d'une session (ou un peu plus); et
- cookies de partage de contenu de plug-in social tiers, pour les membres connectés d'un réseau social.

Bien qu'ils soient exclus du consentement, ces cookies non essentiels restent des à caractère personnel, et il faut toujours une base légale pour les utiliser. Le traitement effectué dans l'intérêt légitime du responsable du traitement constituerait la base juridique la plus appropriée, qui doit être indiquée dans la déclaration de confidentialité.

ii. Cookies non essentiels (sous réserve de consentement)

Selon le WP29, les cookies non essentiels nécessitent un consentement. Il s'agit notamment des éléments suivants :

- les cookies de suivi des plug-ins sociaux ;
- les cookies publicitaires de tiers ; et
- analyse de première partie.

Lorsque le consentement de plusieurs cookies est requis, l'utilisateur doit se voir présenter une option « **Rejeter tout** », en particulier lorsque l'option « **Accepter tout** » est présentée de manière égale.

Dans la mesure du possible, le système doit être capable de préserver les preuves que le consentement a effectivement été accordé, et ces preuves doivent continuer à être conservées aussi longtemps que le traitement fondé sur le consentement a lieu (conformément au principe de responsabilité).

b. Minimisation des données

Selon ce principe, lorsque l'objectif du traitement peut être atteint avec peu de quantités ou moins de données personnelles intrusives, de grandes quantités ou des données plus intrusives ne doivent pas être utilisées. Ainsi, la minimisation doit être à la fois qualitative et quantitative. Voici quelques exemples pratiques.

- Une caméra de surveillance est destinée à prendre uniquement des photos et des vidéos de ceux qui entrent dans un local ou un lieu donné. Par conséquent, il devrait lui être impossible de procéder à l'enregistrement vocal, car il serait considéré comme disproportionné.
- En ce qui concerne une plate-forme en ligne, il convient de veiller à ce que la personne concernée n'ait pas d'espace pour saisir des informations inutiles. Un portail de recrutement ne devrait pas obliger les candidats à télécharger leurs photos, puisque seules les compétences, les qualifications et l'expérience seraient évaluées, et non l'apparence.
- En outre, l'âge d'une personne (par exemple, 15 ans) devrait être préféré à sa date de naissance, car la date de naissance est plus intrusive que l'âge, bien qu'ils soient tous deux considérés comme des données personnelles (alors que la tranche d'âge ne l'est pas). Dans une classe donnée, par exemple, la date de naissance d'un élève donné l'identifierait de manière unique, alors que de nombreux élèves de la classe peuvent avoir le même âge.

- Pour s'authentifier via un numéro de téléphone mobile, seuls les trois derniers chiffres doivent être divulgués aux utilisateurs au lieu du numéro de téléphone mobile complet. Cela ne s'applique pas seulement aux numéros de téléphone, mais aussi aux comptes bancaires ou aux données similaires, car le masquage de la plupart des chiffres de ces données empêche les divulgations à des personnes autres que la personne concernée. Cela s'applique également aux adresses e-mail, où seules les trois premières lettres doivent être affichées.
- Exiger son domaine d'activité au sens large serait plus approprié que d'exiger que l'on précise sa profession.

La minimisation des données est généralement obtenue en combinant des données personnelles avec des données anonymes, plutôt que d'utiliser uniquement des données personnelles.

c. Limitation de la conservation et droit à l'effacement

Il n'est pas permis de traiter ou de stocker des données personnelles plus longtemps que nécessaire.

Le système doit garantir qu'une fois l'objectif du traitement atteint, les données doivent être automatiquement effacées par les moyens techniques suivants:

- faciliter la programmation de la suppression automatique pendant une certaine période;
- dans le cas d'une plateforme en ligne, il convient de veiller à ce que les données des utilisateurs qui n'ont pas accédé à leur compte pendant une certaine période soient automatiquement supprimées après en avoir informé ces utilisateurs ; et
- la suppression doit être définitive.

Parallèlement à ce principe, il existe le droit à l'effacement, qui permet aux personnes concernées de faire supprimer leurs données à tout moment. Le système doit donc permettre aux personnes concernées de supprimer facilement leurs comptes, y compris toutes les données à caractère personnel qu'ils contiennent. Un système qui ne prévoit pas ces possibilités n'est pas adapté.

d. Exactitude des données et droit de rectification

Pour mettre en œuvre ce principe et ce droit, le système doit :

- traiter uniquement les données factuellement correctes, y compris l'heure correcte, l'emplacement correct, et s'assurer qu'il est impossible de falsifier ces informations;
- permettre à la personne concernée de corriger des données inexactes ou obsolètes; et
- permettre aux candidats de mettre à jour les informations qu'ils ont soumises précédemment (par exemple, les documents de demande d'emploi).

Le traitement de données inexactes peut avoir un effet préjudiciable sur la personne concernée, car elle peut se voir refuser un service ou être faussement impliquée dans des situations qui ne la concernent pas, en raison de ces informations inexactes (par exemple, des données de localisation inexactes montrant sa présence sur une scène de crime).

e. Transparence

Le système doit fournir des informations sur tous les aspects du traitement à la personne concernée.

- L'utilisateur a besoin de savoir quelles données sont collectées (traitées) et comment, pourquoi et par qui elles sont collectées, et comment contacter le responsable du traitement. Où elles sont stockées, pendant combien de temps, qui y a accès, s'il est obligé de fournir ces données et les conséquences de ne pas les fournir.
- Il / elle doit également savoir s'il existe des transferts de données en dehors de l'UE et quelles mesures sont en place pour assurer la sécurité de ces données.
- Les droits de la personne concernée doivent également lui être communiqués, y compris les droits à l'effacement, à la rectification, à l'opposition au traitement, au retrait du consentement, à la plainte auprès de l'autorité de contrôle compétente, etc.).
- Les informations peuvent être fournies par le biais d'avis de confidentialité et de symboles superposés. Le Data HelpDesk vous aidera volontiers à rédiger un avis de confidentialité.
- L'information doit être suffisamment explicite, dans un langage simple, pour que même les personnes sans connaissances techniques puissent la comprendre.

- Les informations sur tout ce qui pourrait surprendre l'utilisateur doivent d'abord être portées à l'attention de l'utilisateur.

Tout traitement de données à l'insu de l'utilisateur n'est pas autorisé.

f. Intégrité et confidentialité

Le système traite les données de manière à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dommages accidentels en mettant en œuvre des mesures techniques et organisationnelles appropriées, telles que:

- le chiffrement (de bout en bout) pendant la transmission des données; si le serveur n'est pas dans l'UE : chiffrement des données au repos ;
- la pseudonymisation des données personnelles ;
- la sécurisation de l'accès à distance aux bases de données (par exemple via HTTPS ou d'autres protocoles appropriés);
- la protection des comptes avec un mot de passe sécurisé (longueur minimale, caractères spéciaux, etc.) ou une authentification à deux facteurs;
- l'amélioration ou la mise à jour des dispositifs de sécurité; et
- la certification du système conformément aux NORMES, si une certaine norme est disponible ou nécessaire.

Ces mesures doivent tenir compte de l'état de la technique, du coût de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques associés.

g. Portabilité des données

Si cela est techniquement possible, le système de traitement des données permet à la personne concernée de transférer facilement ses données à un autre prestataire de services ou à d'autres systèmes de traitement.

h. Les droits de restreindre ou de s'opposer au traitement

Le système devrait également être conçu de manière à permettre de suspendre le traitement des données à caractère personnel, sans nécessairement supprimer ces données. Cela peut être réalisé par la désactivation de son profil, soit par le responsable du traitement, soit par la personne concernée elle-même. En effet, la personne concernée a le droit de restreindre le traitement ou de s'opposer à un tel traitement dans certaines circonstances, ce qui, après clarification ou respect de certaines exigences, peut conduire à la reprise de l'activité de traitement, donc au rétablissement du profil désactivé. Pendant cette désactivation ou suspension du traitement, les données à caractère personnel doivent être bien conservées telles quelles, mais invisibles et inaccessibles.

i. Autres considérations

Il convient de noter que nous, les responsables du traitement, sommes tenus d'engager uniquement des processeurs fiables pour traiter les données personnelles en notre nom. À cet égard, vous devriez demander conseil sur la manière de choisir et d'engager contractuellement les fournisseurs de services d'hébergement et de maintenance de l'outil numérique. Vous seriez également orienté sur la façon de soumettre un registre des activités de traitement. Ces exigences sont applicables lorsque ledit outil sera utilisé par la GIZ, et non par un partenaire local.