**Annexe au contrat relative au traitement de données en sous-traitance en vertu de l’article 28 du RGPD**

**Numéro de contrat :**

**Contractant (nom, adresse, pays) :**

**Contenu**

* Clauses 1 à 11
* [Appendice I : Description du traitement](#A1)
* [Appendice II : Liste des sous-traitants ultérieurs](#A2)
* [Appendice III : Mesures techniques et organisationnelles (MTO)](#A3)

**Clause 1 : Objet et champ d’application**

1. La présente annexe au traitement de données en sous-traitance (ci-après dénommée « clauses ») a pour objet de garantir la conformité avec l’article 28, paragraphes 3 et 4 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (**règlement général sur la protection des données**).
2. La GIZ en tant que responsable du traitement et le contractant en tant que sous-traitant (ci-après dénommés « les parties ») ont accepté les présentes clauses afin de garantir le respect des dispositions de l’article 28, paragraphes 3 et 4 du règlement (UE) 2016/679.
3. Les présentes clauses s’appliquent au traitement des données à caractère personnel tel que décrit à l’appendice I.
4. Les appendices I à III font partie intégrante des clauses.
5. Les présentes clauses sont sans préjudice des obligations auxquelles la GIZ est soumise en vertu du règlement (UE) 2016/679.
6. Les présentes clauses ne suffisent pas à elles seules pour assurer le respect des obligations relatives aux transferts internationaux conformément au chapitre V du règlement (UE) 2016/679. Si des données à caractère personnel sont transférées par la GIZ au contractant vers un pays tiers, ce transfert de données doit alors reposer sur un fondement juridique. En l’absence de décision d’adéquation en vertu de l’article 45 ou de garanties appropriées en vertu de l’article 46 du règlement (UE) 2016/679 et faute de dérogation applicable à une situation particulière visée à l’article 49 dudit règlement, un accord contraignant sera passé entre la GIZ et le contractant afin de constituer un fondement juridique. Ledit accord s’inscrit dans le cadre des clauses types de protection des données visées à l’article 46, paragraphe 1 et à l’article 46, paragraphe 2, point c) du règlement (UE) 2016/679.

**Clause 2 : Invariabilité des clauses**

Les parties s’engagent à ne pas modifier les clauses, sauf en ce qui concerne l’ajout d’informations aux appendices ou la mise à jour des informations qui y figurent. Les ajouts ou les mises à jour d’informations mentionnées dans les appendices ne nécessitent pas la conclusion d’un avenant au contrat et peuvent être convenus sous forme écrite simple.

**Clause 3 : Interprétation**

1. Lorsque des termes définis respectivement dans le règlement (UE) 2016/679 figurent dans les clauses, ils s’entendent comme dans le règlement en question.
2. Les présentes clauses doivent être lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679.
3. Les présentes clauses ne doivent pas être interprétées d’une manière contraire aux droits et obligations prévus par le règlement (UE) 2016/679 ou d’une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

**Clause 4 : Hiérarchie**

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes qui existent entre les parties au moment où les présentes clauses sont convenues ou qui sont conclus ultérieurement, les présentes clauses prévaudront.

**Clause 5 : Description du ou des traitements**

Les détails des opérations de traitement, et notamment les catégories de données à caractère personnel et les finalités du traitement pour lesquelles les données à caractère personnel sont traitées pour le compte de la GIZ, sont précisés à l’appendice I.

**Clause 6 : Obligations des parties**

**6.1 Instructions**

1. Le contractant ne traite les données à caractère personnel que sur instruction documentée de la GIZ, à moins qu’il ne soit tenu d’y procéder en vertu du droit de l’Union ou du droit de l’État membre auquel il est soumis. Dans ce cas, le contractant informe la GIZ de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d’intérêt public. Des instructions peuvent également être données ultérieurement par la GIZ pendant toute la durée du traitement des données à caractère personnel. Une instruction désigne un ordre de la GIZ adressé au contractant par écrit, par voie électronique ou à l’oral en vue d’un traitement des données à des fins spécifiques. Ces ordres doivent être documentés. Les instructions sont définies par les termes de référence dans un premier temps. La GIZ est ensuite en mesure de les modifier, de les compléter ou de les remplacer par une seule instruction individuelle sous une forme documentée.
2. Le contractant informe immédiatement la GIZ si, selon lui, une instruction donnée par la GIZ constitue une violation du règlement (UE) 2016/679 ou d’autres dispositions du droit de l’Union ou du droit des États membres relatives à la protection des données.
3. La GIZ peut exiger à tout moment la publication, la rectification, l’adaptation, l’effacement et la limitation du traitement des données.
4. Le contractant n’est autorisé à communiquer des informations à des tiers ou à la personne concernée qu’après avoir obtenu le consentement explicite et préalable de la GIZ. Le consentement doit être documenté par le contractant.

**6.2 Limitation de la finalité**

Le contractant traite les données à caractère personnel uniquement pour les finalités spécifiques du traitement, telles que définies à l’appendice I, sauf instruction complémentaire par la GIZ.

**6.3** **Durée du traitement des données à caractère personnel**

Le traitement par le contractant n’a lieu que pendant la durée précisée à l’appendice I.

**6.4 Sécurité du traitement**

1. Le contractant met au moins en œuvre les mesures techniques et organisationnelles précisées à l’appendice III pour assurer la sécurité des données à caractère personnel. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l’altération, la divulgation non autorisée de données à caractère personnel ou l’accès non autorisé à de telles données (ci-après dénommée « violation de la protection des données à caractère personnel »). Lors de l’évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l’état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les personnes concernées.
2. Pour des raisons liées au progrès technique, le contractant est autorisé à mettre en œuvre des mesures de substitution adéquates. Ce faisant, le niveau de sécurité ne doit pas descendre en deçà du seuil des mesures définies à l’appendice III. Toute modification substantielle doit être documentée.
3. Le contractant n’accorde aux membres de son personnel l’accès aux données à caractère personnel faisant l’objet du traitement que dans la mesure strictement nécessaire à l’exécution, à la gestion et au suivi du contrat. Le contractant veille à ce que les personnes autorisées à traiter les données à caractère personnel s’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

**6.5 Données sensibles**

Si le traitement porte sur des données à caractère personnel révélant l’origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l’appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d’identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l’orientation sexuelle d’une personne physique, ou des données relatives aux condamnations pénales et aux infractions (ci-après dénommées « données sensibles »), le contractant applique des mesures appropriées et spécifiques qui sont adaptées à la nature particulière des données et aux risques associés. Il peut notamment s’agir de mesures visant à limiter le nombre de personnes ayant accès aux données à caractère personnel ou à garantir la capacité, la confidentialité, l’intégrité, la disponibilité et la résilience des systèmes et des services de traitement.

**6.6 Documentation et conformité**

1. Le contractant traite de manière rapide et adéquate les demandes de la GIZ concernant le traitement des données conformément aux présentes clauses.
2. À la demande de la GIZ, le contractant lui fournit les informations nécessaires à la tenue du registre de toutes les activités de traitement au sens de l’article 30, paragraphe 1 du règlement (UE) 2016/679.
3. Le contractant informe immédiatement la GIZ si des vérifications et des mesures sont prévues par les autorités de contrôle ou si une autorité de contrôle transmet une demande, conduit une enquête ou collecte divers renseignements auprès du contractant dans le cadre de ses compétences.
4. Le contractant met à la disposition de la GIZ toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du règlement (UE) 2016/679. À la demande de la GIZ, le contractant permet également la réalisation d’audits des activités de traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence d’indices de non-conformité. Lorsqu’elle décide d’un examen ou d’un audit, la GIZ peut tenir compte des certifications pertinentes en possession du contractant.
5. La GIZ peut décider de procéder elle-même à l’audit ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du contractant et sont, le cas échéant, effectués moyennant un préavis raisonnable.
6. Les parties mettent à la disposition de l’autorité de contrôle compétente, dès que celle-ci en fait la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

**Clause 7 : Recours à des sous-traitants ultérieurs**

1. Le contractant n’est pas autorisé à sous-traiter à un sous-traitant ultérieur (autres sous-traitants) les opérations de traitement qu’il effectue pour le compte de la GIZ en vertu des présentes clauses sans l’autorisation écrite spécifique préalable de la GIZ. Le contractant soumet la demande d’autorisation spécifique au moins vingt (20) jours avant le recrutement du sous-traitant ultérieur en question, ainsi que les informations nécessaires pour permettre à la GIZ de prendre une décision au sujet de l’autorisation. Lesdites informations comprennent au moins le nom complet, l’adresse et le pays du sous-traitant ultérieur, ainsi qu’une description du traitement des données par celui-ci (y compris l’objet, la nature et la durée). La GIZ approuve le recrutement des sous-traitants ultérieurs figurant à l’appendice II. Les parties tiennent à jour le contenu de l’appendice II.
2. Dans le cas d’une exclusion du recours à des sous-traitants ultérieurs (autres sous-traitants), cette éventualité doit être définie par la GIZ à l’appendice II.
3. Lorsque le contractant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte de la GIZ), il le fait au moyen d’un contrat qui impose au sous-traitant ultérieur au moins les mêmes obligations en matière de protection des données que celles imposées au contractant en vertu des présentes clauses. Le contractant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679.
4. À la demande de la GIZ, le contractant lui fournit la copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d’affaires ou d’autres informations confidentielles, y compris les données à caractère personnel, le contractant peut expurger le texte du contrat avant d’en diffuser une copie.
5. Le contractant demeure pleinement responsable, à l’égard de la GIZ, de l’exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le contractant. Le contractant informe la GIZ de tout manquement du sous-traitant ultérieur à ses obligations contractuelles. Dans ce cas, le contractant est tenu, à la demande de la GIZ, de mettre un terme à tout ou partie du travail du sous-traitant ultérieur ou de rompre la relation contractuelle avec le sous-traitant ultérieur lorsque, et dans la mesure où, cela ne s’avère pas disproportionné.
6. Ne sont pas considérés comme des prestations de sous-traitants en vertu des présentes clauses les services auxquels le contractant recourt auprès de tiers sous la forme d’une prestation annexe visant à favoriser l’exécution d’un marché (services de télécommunications, etc.). Le contractant est cependant tenu de passer des accords contractuels appropriés et conformes à la loi et d’adopter des mesures de contrôle pour assurer également la protection et la sécurité des données de la GIZ dans le cas de prestations annexes externalisées.
7. Le contractant convient avec le sous-traitant ultérieur d’une clause du tiers bénéficiaire selon laquelle – dans le cas où le contractant a matériellement disparu, a cessé d’exister en droit ou est devenu insolvable – la GIZ a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d’effacer ou de renvoyer les données à caractère personnel.

**Clause 8 : Transferts internationaux**

1. L’exécution du traitement des données convenu au contrat a lieu uniquement dans un État membre de l’Union européenne ou dans un autre État partie à l’accord sur l’Espace économique européen.
2. Tout transfert de données vers un pays tiers ou une organisation internationale par le contractant n’est effectué que sur la base d’instructions documentées de la GIZ ou afin de satisfaire à une exigence spécifique du droit de l’Union ou du droit de l’État membre à laquelle le contractant est soumis et s’effectue conformément au chapitre V du règlement (UE) 2016/679.
3. La GIZ convient que lorsque le contractant recrute un sous-traitant ultérieur conformément à la clause 7 pour mener des activités de traitement spécifiques (pour le compte de la GIZ) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du règlement (UE) 2016/679, le contractant et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du règlement (UE) 2016/679 en utilisant les clauses contractuelles types adoptées par la Commission sur la base de l’article 46, paragraphe 2 du règlement (UE) 2016/679, pour autant que les conditions d’utilisation de ces clauses contractuelles types soient remplies.

**Clause 9 : Assistance à la GIZ**

1. Le contractant informe sans délai la GIZ de toute demande qu’il a reçue de la part de la personne concernée. Il ne donne pas lui-même suite à cette demande, à moins que la GIZ ne l’y ait autorisé.
2. Le contractant prête assistance à la GIZ pour ce qui est de remplir l’obligation qui lui incombe de répondre aux demandes des personnes concernées d’exercer leurs droits, en tenant compte de la nature du traitement. Dans l’exécution de ses obligations conformément aux points a) et b), le contractant se conforme aux instructions de la GIZ.
3. Outre l’obligation incombant au contractant d’assister la GIZ en vertu de la clause 9, point b), le contractant aide en outre la GIZ à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le contractant :
4. l’obligation de procéder à une évaluation de l’incidence des opérations de traitement envisagées sur la protection des données à caractère personnel (ci-après dénommée « analyse d’impact relative à la protection des données ») lorsqu’un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques ;
5. l’obligation de consulter l’autorité de contrôle compétente préalablement au traitement lorsqu’une analyse d’impact relative à la protection des données indique que le traitement présenterait un risque élevé si la GIZ ne prenait pas de mesures pour atténuer le risque ;
6. l’obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai la GIZ si le contractant apprend que les données à caractère personnel qu’il traite sont inexactes ou sont devenues obsolètes ;
7. les obligations prévues à l’article 32 du règlement (UE) 2016/679.
8. Les parties définissent à l’appendice III les mesures techniques et organisationnelles appropriées par lesquelles le contractant est tenu de prêter assistance à la GIZ dans l’application de la présente clause, ainsi que la portée et l’étendue de l’assistance requise.

**Clause 10 : Notification de violations de données à caractère personnel**

En cas de violation de données à caractère personnel, le contractant coopère avec la GIZ et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu des articles 33 et 34 du règlement (UE) 2016/679 en tenant compte de la nature du traitement et des informations dont dispose le contractant.

**10.1 Violation de données en rapport avec des données traitées par la GIZ**

En cas de violation de données à caractère personnel en rapport avec des données traitées par la GIZ, le contractant prête assistance à la GIZ :

1. aux fins de la notification de la violation de données à caractère personnel à l’autorité de contrôle compétente, dans les meilleurs délais après que la GIZ en a eu connaissance, le cas échéant (sauf si la violation de données à caractère personnel est peu susceptible d’engendrer un risque pour les droits et libertés des personnes physiques) ;
2. aux fins de l’obtention des informations suivantes qui, conformément à l’article 33, paragraphe 3 du règlement (UE) 2016/679, doivent figurer dans la notification de la GIZ, et inclure, au moins :
   1. la nature des données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d’enregistrements de données à caractère personnel concernés ;
   2. les conséquences probables de la violation de données à caractère personnel ;
   3. les mesures prises ou les mesures que la GIZ propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n’est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu’elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais ;

1. aux fins de la satisfaction, conformément à l’article 34 du règlement (UE) 2016/679, de l’obligation de communiquer dans les meilleurs délais la violation de données à caractère personnel à la personne concernée, lorsque la violation de données à caractère personnel est susceptible d’engendrer un risque élevé pour les droits et libertés des personnes physiques.

**10.2 Violation de données en rapport avec des données traitées par le contractant**

En cas de violation de données à caractère personnel en rapport avec des données traitées par le contractant, celui-ci en informe la GIZ dans les meilleurs délais après en avoir pris connaissance. Cette notification contient au moins :

1. une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d’enregistrements de données à caractère personnel concernés) ;
2. les coordonnées d’un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel ;
3. ses conséquences probables et les mesures prises ou les mesures qu’il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n’est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu’elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

Les parties définissent à l’appendice III tous les autres éléments que le contractant doit communiquer lorsqu’il prête assistance à la GIZ aux fins de la satisfaction des obligations incombant à ce dernier en vertu des articles 33 et 34 du règlement (UE) 2016/679.

**Clause 11 : Non-respect des clauses et résiliation**

1. Sans préjudice des dispositions du règlement (UE) 2016/679, en cas de manquement du contractant aux obligations qui lui incombent en vertu des présentes clauses, la GIZ peut donner instruction au contractant de suspendre le traitement des données à caractère personnel jusqu’à ce que ce dernier se soit conformé aux présentes clauses ou jusqu’à ce que le contrat soit résilié. Le contractant informe rapidement la GIZ s’il n’est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.
2. La GIZ est en droit de résilier le contrat dans la mesure où il concerne le traitement des données à caractère personnel conformément aux présentes clauses si :
3. le traitement des données à caractère personnel par le contractant a été suspendu par la GIZ conformément au point a) et le respect des présentes clauses n’est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d’un mois à compter de la suspension ;
4. le contractant est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du règlement (UE) 2016/679 ;
5. le contractant ne se conforme pas à une décision contraignante d’une juridiction compétente ou de l’autorité de contrôle compétente concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement (UE) 2016/679.

Si la GIZ résilie le contrat pour l’un des motifs énoncés précédemment, la résiliation sera imputable au contractant en vertu du point 5.3.2 des Conditions générales.

1. Le contractant est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé la GIZ que ses instructions enfreignent les exigences juridiques applicables conformément à la clause 6.1, point b), la GIZ insiste pour que ses instructions soient suivies.
2. À la suite de la résiliation du contrat, le contractant renvoie à la GIZ toutes les données à caractère personnel traitées pour son compte et détruit les copies existantes, à moins que le droit de l’Union ou le droit national n’impose de les conserver plus longtemps. Le contractant continue de veiller à la conformité aux présentes clauses jusqu’à la suppression ou à la restitution des données.
3. Les supports de données et les enregistrements de données cédés demeurent la propriété de la GIZ.

**Appendice I :** **Description du traitement**

La sélection suivante a été effectuée par la GIZ. Si le contractant relève des lacunes, des erreurs ou des imprécisions dans le cadre de la procédure de passation ou d’exécution du marché, celles-ci doivent être signalées à la GIZ.

Nature, finalité et durée du traitement

L’objet et la durée du traitement de données en sous-traitance, ainsi que la portée, la nature et la finalité du traitement des données à caractère personnel sont définis par les termes de référence et l’offre soumise par le contractant.

Description détaillée de la portée, de la nature et de la finalité du traitement :

Catégories de personnes concernées dont les données à caractère personnel sont traitées

Collaborateur·rice·s de la GIZ, candidat·e·s compris·e·s

Abonné·e·s aux revues, aux bulletins d’information, etc.

Participant·e·s externes aux manifestations

Participant·e·s aux enquêtes

Visiteur·euse·s des locaux de la GIZ

Visiteur·euse·s de sites Internet

Prestataires de services / Fournisseurs

Interlocuteur·rice·s d’institutions partenaires

Représentant·e·s d’organismes publics et représentant·e·s de gouvernement

Étudiant·e·s / Boursiers

Autres :  Les participant.e.s au programme THAMM Plus

Catégories de données à caractère personnel traitées

Données de base des personnes (nom, date de naissance)

Adresse

Coordonnées (numéro de téléphone, adresse électronique, etc.)

Qualifications (parcours professionnels, CV, etc.)

Données des salarié·e·s (données salariales, coordonnées bancaires, caractéristiques fiscales, etc.)

Données de facturation et de paiement

Données des utilisateur·rice·s (données des navigateurs, adresses IP, cookies, identifiants, etc.)

Données des enregistrements audio et vidéo

Données de déplacement et de localisation

Catégories particulières de données à caractère personnel en vertu de l’article 9 du règlement (UE) 2016/679 (données concernant la santé, données biométriques, données ethniques, religieuses, politiques et philosophiques ou données concernant la vie sexuelle ou l’orientation sexuelle d’une personne physique).

Autres :

**Appendice II :** **Liste des sous-traitants ultérieurs**

Le contractant n’est pas autorisé à sous-traiter à un sous-traitant ultérieur les opérations de traitement qu’il effectue pour le compte de la GIZ en vertu des présentes clauses.

La GIZ approuve le recrutement des sous-traitants ultérieurs suivants :

|  |  |  |  |
| --- | --- | --- | --- |
| Nom | Adresse, y compris le pays | Description du traitement (y compris l’objet, la nature et la durée) | En cas de transfert de données à un pays tiers ou à une organisation internationale : comment le respect du chapitre V du règlement (UE) 2016/679 est-il garanti ? |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Appendice III : Mesures techniques et organisationnelles (MTO), y compris celles visant à garantir la sécurité des données**

Description des mesures de sécurité techniques et organisationnelles mises en œuvre par le contractant (y compris toute certification pertinente) visant à garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

La liste de contrôle ci-dessous énumère de nombreuses mesures techniques et organisationnelles possibles et peut être utilisée à des fins de présentation. Elle n’est pas exhaustive et doit être complétée par le contractant au cas par cas, si nécessaire. Des notes explicatives doivent être ajoutées pour chaque cas afin de fournir une description concrète.

La présentation et la description des mesures techniques et organisationnelles prises par le contractant peuvent être également établies dans un document distinct.

**1. Mesures de pseudonymisation et de chiffrement des données à caractère personnel**

Pseudonymisation des données à caractère personnel qui ne sont plus requises en texte clair

Directive relative à la pseudonymisation

Chiffrement des supports de données

Pseudonymisation des données dans des systèmes de test

Chiffrement des sites Internet (SSL)

Chiffrement des bases de données

Chiffrement des courriels (TLS 1.2 ou 1.3)

Chiffrement des mots de passe et des clés

Chiffrement des appareils portables

|  |
| --- |
| Note explicative : |

**2. Mesures visant à garantir la confidentialité, l’intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement**

Accords de confidentialité avec les collaborateur·rice·s

Obligation des collaborateur·rice·s en matière de protection des données

Accord de non-divulgation (NDA) passé avec des tiers

Supports de stockage externes / Serveur de sauvegarde

Contrats d’assistance conclus avec des tiers

Accords d’externalisation du traitement des données

Recours à des fournisseurs certifiés de nuages

Pare-feu

Logiciel antivirus

Sauvegardes régulières des données

Systèmes redondants

Surveillance des systèmes et des services

Systèmes RAID

Serveur de stockage en réseau (NAS)

Contrats de maintenance

Contrôles réguliers des incidents informatiques

Stockage interne de copies ou sauvegardes

Alimentation sans interruption (ASI)

Détecteurs d’incendie et de fumée

Appareils de surveillance des températures

Équipement de lutte contre l’incendie

Alerte en cas d’accès non autorisé

Répartition de charge

|  |
| --- |
| Note explicative : |

**3. Mesures assurant de disposer de moyens permettant de rétablir la disponibilité des données à caractère personnel et l’accès à celles-ci dans des délais appropriés en cas d’incident physique ou technique**

Sauvegardes régulières de l’ensemble du système

Stockage sur plusieurs systèmes

Concept de sauvegarde des données

Contrôle régulier de la sauvegarde ou de la récupération des données

Contrats d’assistance pour le matériel informatique et contrats de services

Concept de préparation aux situations d’urgence

Sauvegarde externalisée des données

Formation régulière du personnel informatique

|  |
| --- |
| Note explicative : |

**4. Procédures visant à tester, à analyser et à évaluer régulièrement l’efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement**

Contrôles internes

Contrôle des marchés (sélection minutieuse des   
contractants, élaboration précise des contrats, etc.)

Vérification régulière des processus informatiques

Audits réguliers (p. ex. par le·la délégué·e à la protection des données)

Vérification régulière des procédures

Audit des MTO par le·la délégué·e à la protection des données

Contrôles réguliers des collaborateur·rice·s

Réalisation d’analyses d’impact relatives à la protection des données

Contrôle de la conception technique et des préréglages

Système de gestion de la protection des données / Manuel de protection des données

|  |
| --- |
| Note explicative : |

**5. Mesures d’identification et d’autorisation des utilisateur·rice·s**

Authentification à deux facteurs

Authentification par identifiant ou mot de passe

Séparation des rôles du système de test et du système productif

Contrôle régulier des autorisations

Mots de passe du BIOS

Concept d’autorisation

Directive relative à la gestion des appareils portables

Profils utilisateur

Directive relative aux mots de passe

Limitation du nombre d’administrateur·rice·s

Identification de nouveaux·elles collaborateur·rice·s

Séparation des rôles d’utilisateur

Mécanismes de verrouillage automatiques

Identification des collaborateur·rice·s externes au moyen de badges

Gestion des droits par un administrateur

Distinction entre les autorisations

|  |
| --- |
| Note explicative : |

**6. Mesures de protection des données pendant le transfert**

Recours aux technologies de chiffrement

Réseau privé virtuel (VPN)

Enregistrement d’activités et d’événements

Transport via un nuage privé

Documentation des destinataires des données

Chiffrement des courriels (TLS 1.2 ou 1.3)

Vérification de l’identité des destinataires

Utilisation de lecteurs non publics

Transport physique : bacs de transport sûrs

Sélection minutieuse du personnel de transport

|  |
| --- |
| Note explicative : |

**7. Mesures de protection des données pendant le stockage**

Chiffrement des supports de données

Classification des données

Concept d’autorisation

Restriction d’accès

Enregistrement d’activités et d’événements

Portes de sécurité

Limitation du nombre d’administrateur·rice·s

Carte-clé / Accès avec identification par radiofréquence (RFID)

Anonymisation des données

Pseudonymisation des données

Conservation des supports de données en lieu sûr

Pare-feu

|  |
| --- |
| Note explicative : |

**8. Mesures visant à garantir la sécurité physique des sites où les données à caractère personnel sont traitées**

Dispositif d’alarme

Contrôle des personnes / Portier

Protection des gaines de bâtiment

Enregistrement des visiteur·euse·s

Contrôle d’accès automatique

Sélection minutieuse du personnel de nettoyage

Sélection minutieuse du personnel de sécurité

Cartes à puce, transpondeur

Système de fermeture par serrure à code

Obligation de porter les badges d’autorisation

Système de fermeture manuelle

Concept d’accès

Verrouillage d’accès biométrique

Racks de serveur verrouillables

Vidéosurveillance des entrées

Portes dotées d’un bouton du côté extérieur

Barrières photoélectriques / Détecteurs de mouvement

Visiteur·euse·s : toujours accompagné·e·s de collaborateur·rice·s

Serrures de sécurité

Sonnerie avec caméra

Procédure de remise des clés

|  |
| --- |
| Note explicative : |

**9. Mesures visant à garantir l’enregistrement des événements**

Recours à un enregistrement automatique

Établissement de rapports d’événements

Notification avec alerte en temps réel

Enregistrement au niveau des applications

Contrôle automatique des procès-verbaux

Synchronisation des horloges du système

Vérification manuelle et régulière des procès-verbaux

Consolidation automatique des événements

Enregistrement des procès-verbaux dans l’application et envoi automatique à un autre endroit

|  |
| --- |
| Note explicative : |

**10. Mesures visant à assurer la configuration des systèmes, y compris la configuration par défaut**

Directive relative à la gestion des configurations

Processus relatif aux modifications des configurations

Préréglages conformes à la protection des données

Contrôle des configurations par défaut

Définition des configurations par défaut

Configuration par l’administrateur·rice système

Enregistrement des modifications des configurations

Formation régulière des collaborateur·rice·s du service informatique

|  |
| --- |
| Note explicative : |

**11. Mesures de gouvernance et de gestion de l’informatique interne et de la sécurité informatique**

Directive relative à la sécurité informatique

Directive relative à l’administration des systèmes informatiques

Vérifications et audits de la conformité effectués à intervalles réguliers

Registre des installations informatiques

Formation des collaborateur·rice·s à la sécurité des données

Évaluation et contrôle réguliers des systèmes

Attribution claire des rôles et des responsabilités de l’équipe du service informatique

Directives relatives à la gestion des événements

Évaluation des risques et mesures de gestion des risques à tous les niveaux

|  |
| --- |
| Note explicative : |

**12. Mesures de certification / assurance qualité des procédés et produits**

Introduction de la norme ISO 9001 – Management de la qualité

Introduction de la norme ISO 27001 – Management de la sécurité de l’information

Mise en œuvre de la norme ISO 27701 – Management de la protection de la vie privée

Certification RGPD – Gestion de la protection des données

Vue d’ensemble des dispositions applicables aux produits, aux services et aux processus

Identification des normes sectorielles

Audits internes et/ou externes réguliers

Attribution de responsabilités en matière d’audit à des expert·e·s certifié·e·s

Vérification régulière des nouvelles conditions et du renouvellement des certificats

|  |
| --- |
| Note explicative : |

**13. Mesures visant à garantir la minimisation des données**

Identification de la finalité du traitement

Évaluation de la relation entre le traitement et la finalité

Évaluation de la portée et de la qualité des données traitées en fonction de la finalité

Identification des délais de conservation applicables

Effacement sécurisé des données après l’expiration du délai de conservation

|  |
| --- |
| Note explicative : |

**14. Mesures visant à garantir la qualité des données**

Profilage et classification des données

Contrôle des données entrantes ou des nouvelles données

Enregistrement de la saisie ou de la modification des données

Attribution des droits de saisie des données

Conservation des procès-verbaux

Traçabilité des utilisateur·rice·s lors de la saisie et de la modification des données (aucun groupe d’utilisateur·rice·s)

Prévention de doublons

Identification des exigences relatives aux données

Application de mesures visant à garantir la qualité des données

|  |
| --- |
| Note explicative : |

**15. Mesures visant à garantir une conservation limitée des données**

Directive relative à la conservation précisant les rôles

Séparation des données en fonction des délais de conservation

Formations régulières

Évaluation et contrôle réguliers des données enregistrées

|  |
| --- |
| Note explicative : |

**16. Mesures visant à garantir la responsabilité**

Formations / Sensibilisation

Contrôles et examens réguliers

Équipe disponible pour la protection des données

Instruction et soutien aux collaborateur·rice·s

Directives appropriées en matière de protection des données

Conclusion de clauses contractuelles types

Accords de responsabilité conjointe

Réponse aux demandes des personnes concernées

Document de transparence (art. 13 / 14 du RGPD)

Effacement sécurisé des données

Charte de confidentialité documentée

Mesures et rapports d’audit documentés

Implication appropriée du·de la délégué·e à la protection des données

Procédure de consentement spécifique / Conservation des procès-verbaux de consentement

|  |
| --- |
| Note explicative : |

**17. Mesures permettant la portabilité des données et garantissant l’effacement**

Enregistrement dans un format structuré

Surveillance des délais légaux

Transmission par chiffrement de bout en bout

Respect des délais de conservation

Application de mesures permettant la portabilité des données

Gestion des droits des personnes concernées en vertu de l’article 3 du règlement (UE) 2016/679

Garantie d’un effacement sécurisé des données

Garantie d’une destruction sécurisée des supports de données

|  |
| --- |
| Note explicative : |