Mesures de sécurité relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

Le présent document décrit les mesures générales de sécurité organisationnelles et techniques de POST liées au traitement des données à caractère personnel dans le cadre de l'exécution des contrats avec ses clients professionnels

INTRODUCTION

POST met en œuvre un ensemble raisonnable de mesures techniques et organisationnelles visant à garantir un niveau de sécurité approprié des données à caractère personnel traitées par POST pour le compte du client. L'objectif des mesures de sécurité que POST met en place est de protéger les données à caractère personnel des éventuelles violations de 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. Le niveau de sécurité défini varie en fonction du traitement des données à caractère personnel et tient compte de la nature, de la portée, du contexte et des finalités du traitement, du type de données traitées ainsi que des risques identifiés au niveau des droits et libertés des personnes concernées. Ce niveau de sécurité prend également en considération l'état des connaissances et les coûts de mise en œuvre.

1. Mesures visant à garantir la pseudonymisation et le chiffrement des données à caractère personnel

En qualité de responsable du traitement et/ou sous-traitant, POST assure la pseudonymisation et/ou le chiffrement des données à caractère personnel en adoptant des techniques permettant d'anticiper divers scénarios. Il convient d'analyser chaque cas de traitement de données à caractère personnel en fonction des risques associés dans le but de déterminer la technique de pseudonymisation et de chiffrement des données à caractère personnel la plus appropriée.

Identifiant de la mesure	Description de la mesure
1	POST a élaboré une politique de chiffrement des données et de gestion des clés, qui définit les exigences relatives au recours au chiffrement et à la protection des clés cryptographiques.
2	Création et validation d'un certificat signé par une autorité digne de confiance pour chiffrer les données sensibles et sécuriser l'accès Web via HTTPS
3	Des protocoles d'authentification sécurisés sont utilisés le cas échéant (FTPS, LDAPS, SSH, etc.).
4	Par défaut, les données de production comportant des données à caractère personnel réelles ne sont pas utilisées dans l'environnement de test et de développement.
5	Des techniques de pseudonymisation sont appliquées et consistent à séparer les données des identifiants directs afin d'empêcher que des données puissent être reliées à la personne à laquelle elles se rapportent sans informations supplémentaires.
6	Le chiffrement intégral du disque est activé sur les lecteurs du système d'exploitation du poste de travail.
7	L'utilisation de données de production contenant des données à caractère personnel ou toute donnée confidentielle (C3) ou strictement confidentielle (C4) n'est pas autorisée sauf dans les cas suivants : • les données de production C3 et/ou C4 sont supprimées ou modifiées conformément à la norme ISO/CEI 29101 ou • les mesures de sécurité techniques et organisationnelles sont identiques à celles de l'environnement de production. La copie de données de production dans un environnement de test nécessite l'autorisation préalable du propriétaire de l'application. Ces demandes doivent être consignées à des fins d'audit.

	Relatif la norme ISO 27001:2013 - A.15 Cryptographie / A.12 Sécurité liée à l'exploitation

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

En qualité de responsable du traitement et/ou sous-traitant, POST veille à la mise en place d'un contrôle technique et organisationnel visant à garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et services de traitement des données.

Identifiant de la mesure	Description de la mesure
1	La base de données et les applications sont configurées de manière à s'exécuter via un compte séparé, avec des permissions suffisantes sur le système d'exploitation pour pouvoir fonctionner correctement.
2	Les serveurs de base de données et d'applications ne gèrent que les données à caractère personnel dont le traitement est requis conformément aux finalités définies.
3	Des solutions de chiffrement sur des fichiers ou des dossiers spécifiques peuvent être utilisées à l'aide de logiciels ou de matériel informatique.
4	Les disques de stockage sont chiffrés le cas échéant.
5	Les collaborateurs participant au traitement à haut risque des données à caractère personnel sont tenus de respecter des clauses de confidentialité spécifiques (en vertu de leur contrat de travail ou d'un autre acte juridique).
6	POST s'assure que tous les collaborateurs comprennent leurs responsabilités et obligations relatives au traitement des données à caractère personnel. Les rôles et les responsabilités sont précisés lors du processus de préembauche et/ou d'intégration.
7	Avant de prendre leurs fonctions, les collaborateurs sont invités à prendre connaissance de la politique de sécurité de l'entreprise, à s'engager à la respecter et à signer les accords de confidentialité correspondants.
8	POST a défini les principales vérifications et procédures à suivre afin de garantir le niveau requis de continuité et de disponibilité du système informatique traitant les données à caractère personnel (en cas d'incident/violation de données à caractère personnel).
	Relatif à la norme ISO 27001:2013 - A.12 Sécurité liée à l'exploitation / A.15 Relations avec les fournisseurs / A.7 Sécurité des ressources humaines / A.17 Aspects de sécurité de l'information dans la gestion de la continuité de l'activité

3. Mesures visant à permettre de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci en temps opportun en cas d'incident physique ou technique

POST met en œuvre un système de sauvegarde pour la récupération des données à caractère personnel en cas de perte ou de destruction. La fréquence et la nature des sauvegardes dépendront de la nature des données traitées. POST respecte l'article 32 du RGPD en ce qui concerne les « moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci » dans le cadre des obligations de sécurité des données incombant au responsable du traitement ou au sous-traitant.

Identifiant de la mesure	Description de la mesure
1	Les procédures de sauvegarde et de restauration des données sont définies, consignées et liées précisément aux rôles et responsabilités.
2	Les sauvegardes bénéficient d'un niveau approprié de protection physique et environnementale conforme aux normes appliquées aux données d'origine.

Identifiant de la mesure	Description de la mesure
3	L'exécution des sauvegardes est surveillée dans le but de garantir leur exhaustivité.
4	Des sauvegardes complètes sont effectuées régulièrement.
5	Les supports de sauvegarde sont testés régulièrement pour s'assurer qu'ils peuvent être utilisés en cas d'urgence.
6	Des sauvegardes incrémentielles planifiées sont effectuées au moins une fois par jour.
7	Des copies des sauvegardes sont stockées en toute sécurité à différents endroits.
8	Des copies des sauvegardes sont également chiffrées et stockées en toute sécurité hors ligne.
	Relatif à la norme ISO 27001:2013 - A.12.3 Sauvegarde

En cas de violation de données à caractère personnel, POST détermine si celle-ci entraîne, « de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données » (art. 4, point 12, du RGPD). POST s'engage à respecter les obligations visées aux articles 33 et 34 du RGPD en matière de notification d'une violation de données à caractère personnel à l'autorité de contrôle et aux personnes concernées. POST veille également au respect de son obligation au titre de l'article 33 du RGPD relatif à la notification immédiate au responsable du traitement. Dans tous les cas, POST a mis en place des procédures appropriées, non seulement pour la notification des violations de données à caractère personnel, mais également pour le traitement et la gestion globaux de ces situations.

Identifiant de la mesure	Description de la mesure
1	Une politique et des plans de réaction aux incidents comportant des procédures détaillées sont définis dans le but de garantir une réponse efficace et ordonnée aux incidents relatifs à des données à caractère personnel.
2	Les violations de données à caractère personnel sont signalées immédiatement à la direction. Des procédures de notification des violations aux autorités compétentes et aux personnes concernées sont en place, conformément aux articles 33 et 34 du RGPD.
3	Le plan de réaction aux incidents est consigné et comporte notamment une liste des mesures d'atténuation possibles et une répartition claire des rôles.
4	Les incidents relatifs à des données à caractère personnel et les violations de celles-ci sont consignés de façon détaillée (description des événements et mesures d'atténuation mises en place).
	Relatif à la norme ISO 27001:2013 - A.16 Gestion des incidents liés à la sécurité de l'information

4. Processus de test, d'évaluation et d'examen réguliers de l'efficacité des mesures techniques et organisationnelles afin de garantir la sécurité du traitement

Sur le plan technique, POST s'acquitte de cette tâche en mettant en place un certain nombre de mesures techniques, telles que des analyses des vulnérabilités, des tests de pénétration ainsi que des évaluations de sécurité régulières et des audits internes/externes sur les infrastructures et systèmes essentiels. L'objectif principal consiste à identifier les risques éventuels et les points à améliorer.

Identifiant de la mesure	Description de la mesure
1	Dans le cadre du développement, des tests et des validations de la mise en œuvre des exigences de sécurité initiales sont réalisés.

Identifiant de la mesure	Description de la mesure
2	Des analyses des vulnérabilités et des tests de pénétration des applications et des infrastructures sont effectués si nécessaire après l'évaluation de la sécurité de CyberForce préalablement à l'adoption opérationnelle. La mise en œuvre ne sera adoptée que si le niveau de sécurité requis est atteint.
3	Les correctifs logiciels doivent être testés et évalués avant d'être installés dans un environnement opérationnel.
4	Le système de contrôle d'accès doit être en mesure de détecter les mots de passe qui ne respectent pas le niveau de complexité (configurable) requis conformément aux politiques de sécurité de POST et de ne pas autoriser leur utilisation.
5	Les exigences de sécurité sont incluses dans le PPMO (POST Portfolio Management Office), c'est-à-dire le processus de sécurité / confidentialité dès la conception et les documentations définies au niveau du Groupe POST. Tout nouveau projet devra suivre les étapes de sécurité en vue de sa validation.
6	Conformément aux politiques en matière de sécurité de l'information de POST, les processus suivants ont notamment été mis en œuvre : • processus de gestion des vulnérabilités et des correctifs ; • processus de gestion de la configuration ; • processus de journalisation et de surveillance ; • processus de gestion de l'accès logique. Les indicateurs clés de performance (KPI) et de risque (KRI) de ces processus font régulièrement l'objet de rapports à la direction.
	Relatif à la norme ISO 27001:2013 - A.12.6 Gestion des vulnérabilités techniques / A.14.2 Sécurité des processus de développement et d'assistance technique

5. Mesures d'identification et d'autorisation des utilisateurs

POST met en œuvre des mesures de contrôle d'accès et d'authentification de base visant à assurer une protection contre les accès non autorisés au système informatique utilisé dans le cadre du traitement des données à caractère personnel.

Identifiant de la mesure	Description de la mesure
1	Des droits de contrôle d'accès spécifiques sont attribués à chaque rôle (participant au traitement des données à caractère personnel) selon le principe du besoin de savoir (modèle RBAC).
2	Un système de gestion de l'identité et de l'accès (IAM) applicable à tous les utilisateurs accédant au système informatique est mis en place. Le système permet de créer, d'approuver, d'examiner et de supprimer des comptes utilisateurs.
3	L'utilisation de comptes utilisateurs génériques/partagés est interdite par défaut.
4	Un mécanisme d'authentification est en place, permettant l'accès au système informatique (conformément à la politique et au système de contrôle d'accès). Une combinaison nom d'utilisateur/mot de passe est utilisée au minimum. Les mots de passe doivent respecter un certain niveau de complexité (configurable) conformément aux politiques de sécurité du Groupe POST.
5	Le système de contrôle d'accès est en mesure de détecter les mots de passe qui ne respectent pas le niveau de complexité (configurable) requis et de ne pas autoriser leur utilisation.
6	Une politique de mot de passe spécifique est définie et consignée. La politique comprend des exigences relatives à la longueur du mot de passe, à sa complexité, à sa durée de validité, ainsi qu'au nombre autorisé d'échecs de connexion.
7	La séparation des rôles de contrôle d'accès (par exemple, demande d'accès, autorisation d'accès, administration d'accès) est définie et consignée.
8	L'authentification à deux facteurs est utilisée pour tous les accès à distance au réseau POST. Les facteurs d'authentification incluent des mots de passe et un mot de passe à usage unique (OTP).
9	L'authentification de l'appareil est utilisée pour garantir que le traitement des données à caractère personnel s'effectue uniquement via des ressources spécifiques du réseau.
10	Les rôles avec des droits d'accès supérieurs sont définis précisément et attribués à un nombre limité de membres du personnel.
11	L'accès au système informatique s'effectue exclusivement via des appareils et périphériques préalablement autorisés.
	Relatif à la norme ISO 27001:2013 - A.9 Contrôle d'accès / A.9.1.1 Politique de contrôle d'accès

6. Mesures de protection des données lors de leur transmission

POST met en œuvre des mesures de sécurité du réseau pour la protection des données à caractère personnel, tant en ce qui concerne les connexions externes (par exemple à Internet), que l'interconnexion avec d'autres systèmes (externes ou internes) de l'entreprise.

Identifiant de la mesure	Description de la mesure
1	À chaque accès à Internet, la communication est chiffrée via des protocoles de chiffrement (TLS/SSL).
2	L'accès sans fil au système informatique est protégé par chiffrement.
3	Le trafic depuis le système informatique et vers celui-ci est surveillé et contrôlé par des pare-feu et des IDS (systèmes de détection d'intrusion).
4	Le réseau du système d'information est séparé des autres réseaux du responsable du traitement.

Identifiant de la mesure	Description de la mesure
	Relatif à la norme ISO 27001:2013 - A.13 Sécurité des communications / A. 14.1 Exigences de sécurité applicables aux systèmes d'information

7. Mesures de protection des données lors de leur stockage

POST met en œuvre des politiques de sécurité visant à protéger les données pendant leur stockage, notamment en interdisant aux utilisateurs d'effectuer certaines actions susceptibles de compromettre la sécurité du système informatique (par exemple, la désactivation de programmes antivirus ou l'installation de logiciels non autorisés).

Identifiant de la mesure	Description de la mesure
1	Les utilisateurs ne peuvent pas désactiver ou contourner les paramètres de sécurité.
2	Les applications antivirus et les signatures de détection sont configurées quotidiennement.
3	Les utilisateurs ne disposent pas des permissions d'installation d'applications logicielles non autorisées ou de désactivation de logiciels installés.
4	La configuration du système inclut des délais d'expiration de session en cas d'inactivité de l'utilisateur pendant un certain temps.
5	Des mises à jour de sécurité essentielles sont installées régulièrement conformément aux politiques de sécurité du Groupe POST.
6	Le chiffrement complet du disque est activé sur les lecteurs du système d'exploitation du poste de travail.
	Relatif à la norme ISO 27001:2013 - A. 14.1 Exigences de sécurité applicables aux systèmes d'information

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

POST met en œuvre des mesures de sécurité physique concernant les bureaux ainsi que le centre de données où sont traitées les données à caractère personnel.

Identifiant de la mesure	Description de la mesure
1	POST a élaboré une politique de sécurité physique et a désigné un PSO (responsable de la sécurité physique).
2	Les accès physiques sont enregistrés. Le PSO procède à des contrôles réguliers de la sécurité et des accès physiques.
3	Des systèmes de vidéosurveillance sont déployés dans les locaux et le centre de données.
4	Les zones à accès réglementé font l'objet d'examens/de contrôles à intervalles réguliers.
5	Des audits internes et/ou externes des locaux de POST et des mesures de sécurité physique du centre de données sont réalisés chaque année dans le cadre de la certification ISO 27001.
6	Tous les membres du personnel et les visiteurs accédant aux locaux de l'entreprise sont identifiés à l'aide de badges le cas échéant.
7	Des zones sécurisées ont été définies et sont dotées de systèmes de protection appropriés (contrôles des entrées). Un registre physique ou une piste de vérification électronique de tous les accès est conservé(e) en lieu sûr et tenu(e) à jour.

Identifiant de la mesure	Description de la mesure
8	Des systèmes de détection d'intrusion sont installés dans toutes les zones de sécurité.
9	Des barrières physiques sont mises en place, le cas échéant, afin de prévenir tout accès physique non autorisé.
10	Les zones sécurisées inoccupées sont verrouillées physiquement et inspectées à intervalles réguliers.
11	Un système d'extinction automatique d'incendie, un système de climatisation dédié à circuit fermé et un système d'alimentation sans coupure (onduleurs) sont mis en place dans les salles de serveurs.
12	Le personnel du service d'assistance externe bénéficie d'un accès réglementé aux zones sécurisées.
	Relatif à la norme ISO 27001:2013 - A.11 – Sécurité physique et environnementale

9. Mesures visant à garantir l'enregistrement des événements

L'utilisation de fichiers journaux est une mesure de sécurité essentielle qui permet l'identification et le suivi des actions de l'utilisateur (ayant trait au traitement des données à caractère personnel), facilitant ainsi la reddition de comptes en cas de divulgation, modification ou destruction non autorisée de données à caractère personnel. La surveillance des fichiers journaux est une tâche importante et vise à identifier les tentatives internes ou externes éventuelles de violation du système.

Identifiant de la mesure	Description de la mesure
1	Des fichiers journaux sont activés pour chaque système/application utilisé(e) dans le cadre du traitement des données à caractère personnel. Ils doivent inclure tous les types d'accès aux données (consultation, modification, suppression).
2	Les fichiers journaux sont horodatés et protégés de manière appropriée contre les risques de falsification et d'accès non autorisé. Les horloges sont synchronisées sur une seule référence temporelle.
3	Les actions des administrateurs et des exploitants du système, notamment l'ajout/la suppression/la modification des droits des utilisateurs, sont consignées.
4	Il n'est pas possible de supprimer ou de modifier le contenu des fichiers journaux. Outre la surveillance, l'accès aux fichiers journaux doit également être enregistré dans le but de détecter les activités inhabituelles.
5	Un système de surveillance doit traiter les fichiers journaux, générer des rapports sur l'état du système et signaler les alertes éventuelles.
	Relatif à la norme ISO 27001:2013 – A.12.4 Journalisation et surveillance

10. Mesures visant à garantir la configuration du système, notamment la configuration par défaut

Une configuration sécurisée fait référence aux mesures de sécurité mises en œuvre lors de la conception et de l'installation d'ordinateurs et de périphériques réseau dans le but de réduire les vulnérabilités informatiques injustifiées et de prévenir les risques d'exploitation ou les dangers.

Identifiant de la mesure	Description de la mesure
1	POST a établi des directives de configuration visant à renforcer le système.
2	POST a mis en place un processus de gestion de la configuration dans le but de garantir la sécurité des configurations système.

Identifiant de la mesure	Description de la mesure
3	Les configurations des systèmes informatiques essentiels font l'objet de contrôles réguliers visant à garantir leur conformité aux exigences de base, aux normes et aux bonnes pratiques.
	Relatif à la norme ISO 27001:2013 - A.12 Sécurité liée à l'exploitation

11. Mesures relatives à la gouvernance et la gestion internes de la sécurité et des systèmes informatiques

a. Politiques en matière de sécurité de l'information

POST a mis en place un SMSI (Système de Management de la Sécurité de l'Information), qui comprend la politique en matière de sécurité de l'information, ainsi qu'un certain nombre de politiques secondaires abordant des aspects particuliers. Ce cadre recense également des processus connexes en vue de démontrer la conformité aux exigences de contrôle de la norme ISO 27001:2013.

Identifiant de la mesure	Description de la mesure
1	La politique en matière de sécurité de l'information et les politiques secondaires pertinentes sont communiquées au personnel et aux tiers intéressés selon le principe du besoin de savoir.
2	Toutes les politiques en matière de sécurité de l'information de POST font l'objet de contrôles et de mises à jour à intervalles réguliers.
	Relatif à la norme ISO 27001:2013 - A.5 Politiques de sécurité de l'information

b. Organisation de la sécurité de l'information

Identifiant de la mesure	Description de la mesure
1	Les rôles et les responsabilités en termes de sécurité de l'information sont définis dans la politique en matière de sécurité de l'information.
2	Le responsable de la conformité de POST est en lien avec les autorités compétentes à des fins de sécurité. Le délégué à la protection des données de POST est en lien avec l'autorité de protection des données.
3	Différentes fonctions au sein de POST, telles que le responsable de la conformité, le responsable de la sécurité de l'information et le responsable de la protection des données, sont en contact avec des groupes d'intérêts.
4	Un processus d'évaluation de la sécurité de l'information (« sécurité dès la conception ») pour les nouveaux projets et les nouveaux produits a été mis en place à des fins de gestion des risques liés à la sécurité.
5	Une procédure de confidentialité et de sécurité dès la conception est définie et appliquée aux nouveaux projets et produits. Ces processus comprennent une évaluation des risques, des tests de pénétration et des analyses d'impact sur la protection des données.
6	POST a mis en place une politique de gestion des risques et une procédure de gestion des risques opérationnels et de sécurité. Des évaluations régulières des risques opérationnels et de sécurité sont réalisées, en particulier pour les systèmes/environnements informatiques essentiels.
	Relatif à la norme ISO 27001:2013 - A.6 Organisation de la sécurité de l'information

c. Sécurité des ressources humaines

Identifiant de la mesure	Description de la mesure
1	POST a mis en place des procédures d'accueil et de départ du personnel dans toutes les entités de POST, ainsi que des contrôles préalables à l'embauche.
2	Les nouveaux membres du personnel sont soumis à un examen préalable à l'embauche et à un contrôle de leurs antécédents.
3	Le kit de bienvenue des nouveaux collaborateurs comprend : • la politique en matière de sécurité de l'information ; • le livret intitulé « Sécurité de l'information et protection des données personnelles » ; • un document relatif aux exigences de sécurité propres à POST Telecom (en vertu de son agrément de PSF de support et de la certification ISO 27001).
4	La direction de POST impose aux collaborateurs et sous-traitants de respecter les politiques et procédures mises en place.
5	Des contrôles de conformité aux politiques et procédures sont effectués par différents moyens : contrôle annuel de la politique du « clean desk » (espaces de travail épurés) et du « clean screen » (dossiers de l'ordinateur classés et triés), examen des indicateurs clés de performance sur les incidents de sécurité, etc.
6	POST organise des formations et sessions annuelles de sensibilisation à la sécurité pour toutes ses entités, y compris POST Telecom. Des campagnes annuelles contre le phishing sont mises en place pour tester la réaction du personnel.
	Relatif à la norme ISO 27001:2013 - A.7 Sécurité des ressources humaines

12. Mesures de certification/d'assurance de la qualité des processus et des produits

POST Telecom est certifié ISO 27001:2013 pour son Système de Management de la Sécurité de l'Information (SMSI), attestant du haut niveau de maturité des processus de gestion et d'exploitation de son infrastructure dédiée à la fourniture de services gérés (dans les locaux ou sur le cloud), ainsi que de tous les processus de support inhérents à la fourniture de ces services à ses clients. La certification ISO 27001 démontre l'expertise de POST Telecom dans ce domaine et garantit aux clients un niveau élevé de sécurité de leurs solutions gérées et de standardisation des processus de gestion de POST Telecom.

13. Mesures visant à garantir le respect des principes de protection des données

Le respect des droits des clients, des collaborateurs et des partenaires fait partie des valeurs de POST. À cet égard, POST s'attache à traiter les données à caractère personnel conformément à la réglementation et selon des principes de transparence, de déontologie et de respect de la vie privée. POST a défini plusieurs finalités de traitement des données à caractère personnel.

Dans le cadre de sa Politique de protection des données, POST s'engage à ne traiter que les données à caractère personnel appropriées, pertinentes et strictement nécessaires au traitement aux fins des finalités définies.

a. Confidentialité dès la conception/par défaut

Identifiant de la mesure	Description de la mesure
1	POST a défini une politique de confidentialité dès la conception pour tous les nouveaux produits ou toutes les nouvelles activités de traitement impliquant le traitement de données à caractère personnel en qualité de sous-traitant. Cette politique vise à concevoir les processus et les systèmes de façon à limiter la collecte et le traitement (notamment l'utilisation, la divulgation, la conservation, la transmission et la suppression) à ce qui est adéquat, pertinent et nécessaire au regard des finalités identifiées du responsable du traitement.

Identifiant de la mesure	Description de la mesure
2	POST a mis en place une politique globale de conservation des données à caractère personnel visant à garantir que la durée de conservation des données se limite à ce qui est strictement nécessaire au regard des objectifs de ses propres activités de traitement de données pertinentes. La durée de conservation est définie dès la phase projet et en fonction des finalités et des catégories de données à caractère personnel traitées.
3	Des mécanismes de correction des données à caractère personnel et d'anonymisation de celles-ci lorsqu'elles ne sont plus nécessaires sont envisagés dès la phase projet.
4	Les fichiers temporaires créés dans le cadre du traitement des données à caractère personnel sont supprimés (effacés ou détruits) selon des procédures consignées dans un délai défini.
5	Les données à caractère personnel sont transférées sur des réseaux de transmission de données assortis de contrôles appropriés garantissant que les données atteignent leur destination prévue.
	Relatif à la norme ISO 27701:2019 - 7.4 Confidentialité dès la conception et confidentialité par défaut / 8.4 Confidentialité dès la conception et confidentialité par défaut

b. Obligations à l'égard des responsables du traitement

Identifiant de la mesure	Description de la mesure
1	POST a mis en place des systèmes conçus pour détecter en temps opportun les violations de données.
2	POST a mis en place une procédure opérationnelle visant à s'assurer que les (éventuelles) violations de données sont notifiées à ses clients professionnels dans les meilleurs délais.
3	POST a mis en place des procédures opérationnelles visant à aider ses clients professionnels à respecter leurs obligations en tant que responsables du traitement. Exemples : • réalisation d'analyses d'impact relatives à la protection des données (AIPD) ; et • assistance dans le cadre de la gestion des demandes des personnes concernées.
4	Au terme du contrat, les données à caractère personnel sont restituées au client et/ou supprimées de manière sécurisée.
	Relatif à la norme ISO 27701:2019 – 8.3 Obligations à l'égard des DCP

c. Responsabilisation

Identifiant de la mesure	Description de la mesure
1	POST a mis en place un Système de Management de la Protection des Données (SMPD) afin de garantir la responsabilité dans le cadre des activités de traitement des données à caractère personnel et des contrôles associés.
2	POST consigne les activités de traitement réalisées pour le compte de ses clients professionnels, notamment les suivantes : • catégories de traitements réalisés pour le compte de chaque client ; • transferts vers des pays tiers ou des organisations internationales ; et

Identifiant de la mesure	Description de la mesure
	• description générale des mesures de sécurité techniques et organisationnelles.
3	POST dispose d'une liste précise de pays et d'organisations internationales vers lesquels les données à caractère personnel peuvent être transférées.
	Relatif à la nome ISO 27701:2019 – 8.2.6 Enregistrements liés au traitement des DCP / 8.5 Partage, transfert et divulgation des DCP

14. Mesures visant à permettre la portabilité des données et garantir leur effacement

POST a défini des politiques et des mesures visant à garantir la suppression ou la destruction irréversible des données à caractère personnel de façon à ce qu'il soit impossible de les récupérer. Les méthodes utilisées varient en fonction de la technologie de stockage, dont les copies papier. Lors de l'élimination d'équipements obsolètes ou redondants, POST s'assure que toutes les données précédemment stockées sur les appareils ont fait l'objet d'une suppression préalable.

Identifiant de la mesure	Description de la mesure
1	L'écrasement logiciel (format sécurisé conforme à la politique POST) est effectué sur tous les supports avant leur élimination. Dans les cas où cette opération ne serait pas possible (CD, DVD, etc.), il est procédé à une destruction physique.
2	Les documents papier utilisés pour stocker des données à caractère personnel doivent être déchiquetés.
3	En cas de recours aux services d'un tiers pour éliminer en toute sécurité des supports ou des documents papier, un contrat de prestation de service est conclu et un certificat de destruction des documents est produit, le cas échéant.
4	Après l'effacement du logiciel, des mesures matérielles supplémentaires telles que la démagnétisation doivent être effectuées. Selon le cas, la destruction physique est également à envisager.
	Relatif à la norme ISO 27001:2013 - A. 8.3.2 Élimination des supports / A. 11.2.7 Élimination sécurisée ou réutilisation des équipements

15. Pour les transferts à destination de sous-traitants, précisez également les mesures techniques et organisationnelles spécifiques à prendre par le sous-traitant pour pouvoir fournir une assistance au responsable du traitement

Identifiant de la mesure	Description de la mesure
1	POST a mis en place une politique de gestion des fournisseurs pour gérer ses fournisseurs et consultants externes.
2	Tous les sous-traitants signent des accords de confidentialité qui définissent leurs responsabilités en matière de protection de toutes les informations de POST (p. ex. : données à caractère personnel, infrastructures…).
3	Les sous-traitants suivent chaque année une formation de sensibilisation à la sécurité.
4	Les exigences de sécurité relatives aux prestations externalisées sont définies dans le contrat conclu entre POST et ses fournisseurs. Des réunions d'examen des fournisseurs sont organisées à intervalles réguliers pour gérer les services externalisés, notamment les aspects de sécurité.
	Relatif à la norme ISO 27001:2013 - A.15 : Relations avec les fournisseurs