Schweizerisches Kompetenzzentrum für den Justizvollzug
Centre suisse de compétences en matière d'exécution des sanctions pénales
Centro svizzero di competenze in materia d'esecuzione di sanzioni penali

Règlement interne relatif à la protection et à la sécurité des données

Version 1.0 / janvier 2026

Route de l'Ancienne-Papeterie 210 | 1723 Marly, Suisse
+41 26 425 44 00 | info@cscsp.ch

www.cscsp.ch

Table des matières

1 Préambule

Le Conseil de fondation approuve et adopte le présent règlement afin d'assurer la conformité des traitements de données aux prescriptions légales et réglementaires, notamment la Loi fédérale sur la protection des données (LPD), ses ordonnances d'application, ainsi que, le cas échéant, lorsque pertinent, le Règlement général sur la protection des données (RGPD) ; ou éventuellement le droit cantonal.

2 Dispositions générales

Art. 1 - Objectif et bases légales

1 Le présent règlement définit les principes et procédures de base ainsi que la manière dont les collaboratrices et collaborateurs du CSCSP doivent traiter les données personnelles dans l'accomplissement de leurs tâches.

2 L'objectif est de protéger la personnalité et les droits fondamentaux de toutes les personnes dont le CSCSP traite les données – en particulier les participant·e·s aux formations et perfectionnements, les participant·e·s à la formation dans l'exécution des peines (Fep), les organisations partenaires, les participant·e·s à des recherches, les mandant·e·s et les collaboratrices et collaborateurs.

3 Le traitement des données personnelles par le CSCSP repose sur l'art. 13 de la Constitution fédérale (Cst.), la Loi fédérale sur la protection des données (LPD) et ses ordonnances d'application, les Statuts de la Fondation, la Convention de prestations, les dispositions cantonales. Il est complété par un document général plus détaillé « Document de base sur la protection des données »[1], lequel fournit des explications et précisions supplémentaires.

Art. 2 – Champs d'application matériel et personnel

1 Le règlement s'applique à tout traitement de données personnelles effectué par le CSCSP dans le cadre de ses missions, quel que soit le support utilisé (papier, électronique, audiovisuel ou autres), le procédé employé ou les données traitées.

2 Il s'applique à l'ensemble du personnel du CSCSP, y compris les chargé·e·s de cours, intervenant·e·s, employé·e·s temporaires, apprenti·e·s, stagiaires et personnes mis·e·s à disposition, ainsi qu'aux partenaires externes, y compris les mandataires et les autres partenaires contractuels.

3 Les collaboratrices et collaborateurs externes du CSCSP qui accomplissent leurs tâches auprès des établissements pénitentiaires et des institutions dans les cantons pour le compte du CSCSP sont soumis au présent règlement et au droit cantonal du canton concerné lorsque celui-ci est le responsable du traitement.

Art. 3 – Définitions

Aux fins du présent règlement on entend par :

a. **données personnelles** : toutes les informations qui se rapportent à une personne physique identifiée ou identifiable, directement ou indirectement ;

b. **personne concernée *:*** il s'agit de la personne physique dont les données personnelles font l'objet d'un traitement par le CSCSP ;

c. **données personnelles sensibles (données sensibles)** : constituent une catégorie particulière de données personnelles, qui, en raison du risque accru d'atteinte aux droits de la personnalité bénéficient d'une protection renforcée :

[1] Voir annexe 1 : document de base

cela concerne des données sensibles au sens strict listées à l'art. 5 let. c LPD :

- les données sur les sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales,
- les données sur la santé, la sphère intime ou l'origine raciale ou ethnique,
- les données génétiques,
- les données biométriques identifiant une personne physique de manière univoque,
- les données sur des poursuites ou sanctions pénales et administratives,
- les données sur des mesures d'aide sociale ;

ainsi que des données considérées comme telles dans les listes d'activités du CSCSP, lesquelles sont traitées dans la pratique comme des données sensibles en raison de leur caractère particulièrement digne de protection ;

d. **traitement** : toute opération ou ensemble d'opérations relatives à des données personnelles – quels que soient les moyens et les support utilisés (électronique, manuel ou combiné) – notamment la collecte, l'enregistrement, la conservation, la communication, l'archivage, l'effacement ou la destruction des données ;

e. **communication** : le fait de transmettre les données personnelles, de les rendre accessibles, peu importe le moyen, la durée et le but ;

f. **externalisation** : une forme qualifiée de sous-traitance impliquant l'utilisation de ressources informatiques accessibles à distance à travers un réseau de communication, pour stocker, traiter et partager des données (informatique en nuage) ;

g. **responsable du traitement** : la fondation CSCSP, représentée par sa direction, qui détermine les finalités et les moyens du traitement des données personnelles et assure la conformité avec la LPD ;

h. **consentement** : manifestation de volonté libre, spécifique, éclairée, par laquelle la personne concernée accepte que des données la concernant fassent l'objet d'un traitement ;

i. **sous-traitant** : la personne physique ou morale qui traite des données pour le compte du CSCSP ;

j. **violation de la sécurité des données personnelles** : tout incident entraînant de manière accidentelle ou illicite la perte des données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données ;

k. **anonymisation** : l'anonymisation d'une donnée permet d'empêcher l'identification de la personne physique concernée ;

l. **pseudonymisation** : consiste à traiter les données personnelles de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires ;

m. **listes des activités** : désigne l'ensemble des opérations du CSCSP impliquant le traitement de données personnelles, établies par domaine ou département[2].

Art. 4 – Catégories de données personnelles traitées par le CSCSP

1 Le CSCSP traite, selon ses activités, les types de données personnelles suivants :

a. **Formations de base, de cadres et continue** : données relatives aux participante·e·s aux cours, aux chargé·e·s de cours, aux examens ainsi qu'aux supports de cours ;

b. **Recherche et développement** : données de projet anonymisées ou pseudonymisées, coordonnées des partenaires de projet ;

c. **Ressources humaines** : données personnelles de base, données relatives aux rapports de travail ;

d. **Communication et administration** : correspondance, listes d'adresses, procès-verbaux de séances, lettres d'information (newsletters) ;

[2] Voir annexe 2 : listes des activités du CSCSP

e. **Données informatiques et d'utilisation** : informations relatives aux journaux d'accès et fichiers journaux techniques (logfiles) ;

f. **Formation dans l'exécution des peines :** données relatives aux personnes détenues, aux examens et support de cours ainsi qu'aux enseignant·e·s.

2 Les données personnelles particulièrement sensibles (par exemple : données relatives à la santé, extrait du casier judiciaire) ne peuvent être traitées que si la loi l'autorise expressément ou si la personne concernée a donné son consentement.

3 Principes régissant le traitement des données

Art. 5 – Principes généraux de la protection des données

Dans l'exécution de leurs tâches, les personnes qui traitent des données doivent toujours respecter les principes suivants :

1 **base légale :** lors de l'exécution d'un processus impliquant le traitement de données personnelles, la personne en charge de l'opération doit s'assurer que ce traitement repose sur une base légale, est directement lié aux missions du CSCSP, ou s'appuie sur le consentement explicite de la personne concernée ;

2 **limitation des finalités** : leur collecte s'effectue uniquement pour des finalités déterminées, explicites et légitimes, liées aux activités du CSCSP ;

3 **le principe de minimisation** : seules les données strictement nécessaires à la finalité du traitement sont collectées et conservées ;

4 **exactitude et actualisation** : lors d'une opération de traitement des données personnelles, la personne en charge de l'opération s'assure qu'elles sont exactes, complètes et tenues à jour au regard de la finalité de leur traitement. Toute inexactitude constatée doit être corrigée sans délai ;

5 **durée de conservation et suppression** :

a. les données ne sont conservées que pendant la durée nécessaire à la réalisation du but du traitement ;

b. à l'échéance de cette période, elles sont détruites, anonymisées ou effacées de manière sécurisée, ou archivées selon les dispositions légales, sauf consentement contraire de la personne concernée ;

c. les durées applicables à chaque catégorie de données sont fixées dans la liste[3] des activités du CSCSP résumées dans une annexe spécifique intitulée : tableau[4] des durées de conservation des données ;

d. l'effacement ou la destruction des données doit être effectuée sous le contrôle de la Conseillère ou du Conseiller à la protection des données ou des archives, et documentés.

6 **Sécurité des données**
Toutes les personnes en charge d'opérations de traitement de données sont tenues de :

a. respecter strictement les directives de sécurité informatique ;

b. signaler immédiatement toute activité suspecte ou tout incident de sécurité à it-support@cscsp.ch;

c. enregistrer les données uniquement sur les systèmes mis à disposition par le CSCSP ;

d. utiliser les moyens de communication sécurisés lors de la transmission des documents confidentiels ;

e. traiter les données personnelles de manière diligente.

[3] Voir annexe 2 : liste des activités de traitement
[4] Voir annexe 3 : tableau durée de conservation

Art. 6 – Proportionnalité, bonne foi et transparence

1 Toute collecte et tout traitement de données doivent se limiter à ce qui est strictement nécessaire à la réalisation du but poursuivi.

2 Lors de la collecte, les personnes en charge de l'opération informent les personnes concernées de manière claire et complète, au moyen du formulaire[5] idoine sur la nature des données collectées et l'utilisation.

3 Aucune donnée personnelle ne peut être utilisée à des fins incompatibles avec la finalité initiale du traitement, sauf consentement de la personne concernée ou base légale expresse.

4 Organisation, responsabilités internes et gestion responsable des données au quotidien et principes

4.1 Organisation et responsabilités internes

Art. 7 – Responsabilité générale de la Direction

1 La Direction du CSCSP assume la responsabilité générale et édicte, par le biais d'une directive[6], les lignes directrices d'application concrète dont chaque personne en charge de traiter des données est tenue de prendre connaissance et de signer. La signature de cette directive atteste de la compréhension et de l'engagement de la personne concernée à respecter les dispositions qui y sont énoncées.

2 Elle veille à ce que les personnes soient dûment informées de leurs obligations en matière de traitement et de sécurité des données et les intègrent dans tous les processus internes.

3 Les personnes responsables d'équipe et celles qui supervisent les interventions de partenaires externes veillent également à ce que les personnes en charge de traiter des données ne disposent que des droits d'accès nécessaires.

Art. 8 – Conseillère ou conseiller à la protection des données

1 La Conseillère ou le Conseiller à la protection des données (ci-après : CPD) et le service informatique (ICT) soutiennent et supervisent la mise en œuvre et la mise à jour du règlement.

2 La Conseillère ou le Conseiller à la protection des données exerce ses fonctions de manière indépendante, et rapporte directement à la Direction.

Art. 9 – Responsabilités individuelles des collaboratrices et collaborateurs

1 **Obligation générale**
Chaque personne en charge de traiter des données est tenue de respecter les principes de protection des données dans l'exercice de ses fonctions, d'assurer la confidentialité des informations traitées et de veiller à ce que tout traitement soit conforme aux directives internes du CSCSP.

2 **Devoir de vigilance**
Les personnes en charge de traiter des données doivent manipuler les données personnelles avec soin et prévenir tout risque d'accès non autorisé, de perte, de modification ou de destruction. Elles signalent sans

[5] Voir annexe 4 : formulaire relatif au devoir d'information
[6] Voir annexe 5 : directive d'application du règlement sur la protection des données.

délai, toute situation présentant un risque ou un incident de sécurité à la ou au supérieur·e hiérarchique, au service ICT, à la Conseillère ou au Conseiller à la protection des données.

3 **Confidentialité**
Il est strictement interdit aux personnes en charge de traiter des données de divulguer, sans autorisation, à des tiers, des informations et données personnelles auxquelles ils ont accès dans le cadre de leurs fonctions.

4 **Utilisation conforme des outils numériques**
Les outils informatiques et les technologies d'intelligence artificielle doivent être utilisés principalement à des fins professionnelles. Ils peuvent être utilisés à titre privé dans le strict respect des directives internes relatives à la sécurité de l'information et à la protection des données.

5 **Principe du besoin d'en connaître**
Les données personnelles ne doivent être consultées, utilisées ou partagées que dans la mesure strictement nécessaire à l'accomplissement des tâches professionnelles et uniquement dans le cadre des finalités pour lesquelles elles ont été collectées.

6 **Responsabilité individuelle**
Chaque personnes en charge de traiter des données demeure responsable de l'usage qu'elle fait des données personnelles. Elle doit veiller à l'intégrité, à la disponibilité et à la traçabilité des informations traitées.

Art. 9a – Principe de précaution

Lorsqu'une personne en charge de traiter des données a un doute sur la légitimité d'un accès, d'un partage ou d'une demande de communication de données, elle doit s'abstenir d'ouvrir ou partager les informations et solliciter immédiatement conseil auprès de la ou du supérieur·e hiérarchique, du service informatique ou de la Conseillère ou le Conseiller à la protection des données.

Art. 10 – Responsabilité des chargé·e·s de cours, intervenant·e·s et mandataires

1 Les chargé·e·s de cours, intervenant·e·s, expert·e·s et mandataires sont soumis·e·s aux mêmes obligations de confidentialité, de protection des données que le personnel interne et s'engagent par écrit à les respecter.

2 Tout manquement à ces obligations peut entraîner la suspension du mandat ou d'autres des mesures.

Art. 11 – Sous-traitants et prestataires externes

1 Lorsqu'un traitement de données est confié à un prestataire externe, celui-ci agit exclusivement sur mandat écrit du CSCSP. Il ne peut effectuer aucune sous-traitance secondaire sans l'autorisation préalable du CSCSP.

2 Le contrat de sous-traitance définit la finalité, la nature et la durée du traitement, précise les obligations de confidentialité et de sécurité équivalentes à celles du CSCSP et garantit que les données ne soient ni transmises ni utilisées à d'autres fins.

3 Le CSCSP demeure le responsable du traitement, même lorsqu'il est exécuté par un tiers.

4.2 Gestion responsable des données au quotidien

Art. 12 – Gestion responsable des données au quotidien

1 Toutes les personnes en charge de traiter des données sont tenues d'appliquer activement le présent règlement dans l'exécution de leurs activités professionnelles au quotidien :

2 **Données électroniques**

a. seuls les outils, logiciels, applications et plateformes mis à disposition ou expressément approuvés par le CSCSP doivent être utilisés pour l'accomplissement des tâches professionnelles ;

b. les données confidentielles doivent être enregistrées uniquement sur SharePoint ou d'autres systèmes autorisés par le CSCSP ;

c. l'utilisation de services cloud privés et de clés USB personnelles pour des tâches professionnelles n'est pas autorisée ;

d. les mots de passe doivent être sûrs, confidentiels et régulièrement modifiés selon les dispositions de la directive ICT sur l'utilisation des outils informatiques ;

e. les courriels contenant des données confidentielles doivent être sécurisés lors de la transmission ;

f. toute transmission de données personnelles doit être approuvée par la Conseillère ou le Conseiller à la protection des données.

3 **Données sur support matériel (papier)**

a. les documents comportant des données personnelles doivent être conservés en lieu sûr, sous clé ou dans un espace avec un accès restreint ;

b. les impressions ou copies non nécessaires doivent être éliminées de manière sécurisée.

4 **Données des réunions et conversations**

a. les informations confidentielles ne doivent en aucun cas être discutées ou échangées dans des espaces publics, ni communiquées à des personnes non autorisées ;

b. il est strictement interdit de transmettre des données sensibles ou des informations personnelles par des services de messagerie, de discussion ou de partage non sécurisés.

5 **Travail en dehors du bureau**

a. lors du télétravail ou des déplacements professionnels, les personnes en charge de traiter des données doivent assurer la protection visuelle des écrans, garantir la sécurité des données traitées et limiter l'accès aux seules personnes autorisées ;

b. les appareils mobiles utilisés dans le cadre professionnel (ordinateurs portables, tablettes, téléphones, etc.) doivent être protégés par un code PIN, un mot de passe sécurisé ou une authentification biométrique.

Art. 13 – Accessibilité et traitement des données sur SharePoint

1 **Système central de gestion et d'archivage électronique - principe**

a. **le SharePoint du CSCSP** constitue le système central de travail, de gestion et d'archivage des documents électroniques. Il est utilisé pour le stockage, le partage et la conservation des informations dans le cadre des activités institutionnelles ;

b. l'accès aux données et documents électroniques à caractère purement informatif, ne contenant aucune donnée personnelle, et dont les finalités de traitement ne se rapportent pas à des personnes identifiées ou identifiables, est ouvert à l'ensemble du personnel du CSCSP.

2 **Restrictions d'accès**

a. chaque domaine, département spécialisé ou service dispose sur SharePoint d'un fichier pour les données et documents contenant des informations personnelles, confidentielles ou sensibles avec des droits d'accès clairement définis et régulièrement mis à jour ;

b. l'accès à ces données et documents est strictement limité aux personnes dûment autorisées, en fonction de leurs attributions, responsabilités ou besoins opérationnels. Cet accès est encadré par des droits définis, contrôlés et révisés régulièrement par le ou la responsable du domaine concerné en collaboration avec le service informatique ;

c. les droits d'accès sont attribués de manière différenciée, selon le principe du besoin d'en connaître et seules les personnes dont les fonctions l'exigent ont accès aux données nécessaires à l'accomplissement de leurs tâches ;

d. tous les espaces contenant des données personnelles ou des informations confidentielles sont strictement limités à un groupe restreint de personnes autorisées ;

e. les personnes externes telles que les partenaires de projet, chargées et chargés de cours ne peuvent accéder qu'aux espaces spécifiquement autorisés et définis à cet effet par le CSCSP.

3 **Gestion et contrôle des droits d'accès** - **Rôles et responsabilités**

a. les droits d'accès aux divers autres systèmes, documents et espaces numériques du CSCSP sont attribués en fonction des tâches, responsabilités et fonctions de chaque collaboratrice et collaborateur ;

b. le·la responsable d'équipe ou le·la chef·fe de domaine attribue les droits d'accès et assure leur contrôle régulier, notamment lors de tout changement de fonction, d'affectation ou de départ d'une personne en charge de traiter des données ;

c. le service informatique met en œuvre les mesures techniques et les droits d'accès, tient les journaux d'accès et veille à la sécurité des systèmes concernés. En concertation avec la Direction, il ajuste et modifie les droits d'accès en fonction des besoins opérationnels ;

d. les personnes en charge de traiter des données ne sont pas autorisées à modifier eux-mêmes les partages, les autorisations ou les liens de partage, ni à les transmettre à des tiers, sauf autorisation expresse de la Direction ou du service informatique.

4 **Traitement, gestion des versions et traçabilité des documents**

a. les documents ne peuvent être traités, enregistrés ou archivés que dans les dossiers spécifiquement prévus à cet effet par le CSCSP ;

b. toute modification doit être traçable et permettre la conservation de l'historique des versions afin de garantir l'intégrité et la transparence du traitement ;

c. les documents originaux ne peuvent être supprimés, altérés ou remplacés qu'avec l'autorisation expresse d'une personne compétente ;

5 **Espace confidentiel – Traitement des données particulièrement sensibles**

Les données particulièrement sensibles, notamment les dossiers du personnel, candidatures ou données de recherche comportant des informations personnelles font l'objet des restrictions renforcées suivantes :

a. l'accès à ces données est strictement réservé aux personnes nommément autorisées par la Direction ou la personne responsable du traitement des données ;

b. ces données doivent être enregistrées exclusivement dans des espaces SharePoint sécurisés et restreints, conformément aux directives du service informatique ;

c. aucun enregistrement local, ni transfert de ces données en dehors de SharePoint n'est autorisé sans l'accord explicite du ou de la responsable des données compétent·e pour le cas d'espèce.

6 **Transmission de données**

a. les données personnelles ne peuvent être transmises, rendues accessibles que si : une disposition légale le prévoit, la personne concernée a donné son consentement ou cela est nécessaire à l'accomplissement des missions du CSCSP ;

b. les demandes de transmission de données doivent être adressées à la Conseillère ou au Conseiller à la protection des données ;

c. toutes les autorisations de partage sur SharePoint s'effectuent de manière sécurisée, sont documentées et vérifiées régulièrement.

Art. 14 – Devoir d'informer lors de la collecte des données personnelles

1 Les personnes en charge de traiter des données sont tenues d'informer de manière claire et adéquate les personnes concernées sur la collecte des données personnelles, que celle-ci soit effectuée auprès d'elles ou non.

2 Lors de la collecte, ils ou elles communiquent à la personne concernée, au moins l'identité et les coordonnées du responsable du traitement, la finalité du traitement, et, cas échéant, les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises.

5 Droits des personnes concernées

Art. 15 – Les différents droits des personnes concernées

1 **Droit d'accès :** toute personne concernée a le droit de demander et de savoir si des données la concernant sont traitées par le CSCSP, ainsi que d'obtenir les informations y relatives.

2 **Droit de rectification, d'effacement et de limitation :** elle peut exiger la rectification des données inexactes ou incomplètes la concernant, leur effacement, ou la limitation du traitement dans les cas prévus par la loi.

3 **Droit d'opposition et limitation à la communication :** elle peut aussi, s'opposer à tout moment, au traitement de ses données personnelles.

4 **Droit de consultation sur place** : la personne concernée peut, avec l'accord du CSCSP, exercer son droit d'accès en consultant sur place, dans les locaux du CSCSP, les données sous forme non électroniques la concernant.

5 **Modalités d'exercice des droits** : toute personne concernée qui souhaite exercer un ou plusieurs des droits susmentionnés doit transmettre une demande dans ce sens à datenschutz@skjv.ch, au moyen du formulaire[7] prévu à cette fin. Le CSCSP examine la demande et rend une décision dans un délai de 30 jours.

Art. 16 – Restrictions aux droits des personnes concernées

1 Le CSCSP peut restreindre temporairement les droits des personnes concernées indiqués à l'art. 15 al. 1 à 4 du présent règlement lorsque cela est nécessaire :

a. à l'exécution d'une mission légale ou d'une procédure administrative ou pénale ;

b. à la sauvegarde d'intérêts publics importants, à la protection des droits et libertés d'autrui.

2 Ces restrictions doivent être proportionnées, motivées et documentées. Les personnes concernées sont informées de la restriction et de sa justification, sauf si cette information compromet la finalité poursuivie.

[7] Voir annexe 6 : formulaire demande d'exercer les droits

6 Sécurité et gestion des données

Art. 17 – Principes généraux de sécurité

1 Le CSCSP met en œuvre des mesures techniques et organisationnelles appropriées pour sécuriser et prévenir tout accès non autorisé, toute perte, altération ou divulgation non souhaitée des données.

2 Ces mesures tiennent compte de la nature des données, de la finalité du traitement, des risques identifiés et de l'état de la technique, ainsi que des ressources financières disponibles.

Art. 18 – Mesures de sécurité techniques et organisationnelles

1 Le service informatique gère les identifiants et les droits d'accès selon le principe du besoin d'en connaître, protège le système contre tout incident dommageable.

2 Sous l'angle organisationnel, la Direction prévoit des procédures internes claires en matière de gestion des données ; organise la formation et la sensibilisation régulières du personnel, et documente les incidents et des correctifs effectués.

Art. 19 – Formations et sensibilisation

1 Les formations en matière de protection et de sécurité des données sont obligatoires pour l'ensemble du personnel et les mandataires du CSCSP.

La Conseillère ou le Conseiller à la protection des données organise régulièrement des actions de sensibilisation (séances, communication interne, supports en ligne, guide de bonne pratique) et veille à l'actualisation régulière du contenu des formations et à la tenue d'un registre de participation.

Art. 19a – Intégration et formation des nouvelles personnes en charge de traiter des données

Accueil, information et formation initiales obligatoire
Lors de leur entrée en fonction, les nouvelles personnes en charge de traiter des données reçoivent par écrit, une information complète sur les règles applicables en matière de protection des données et de sécurité de l'information. Elles sont tenues de suivre une formation initiale obligatoire.

Art. 20 – Analyse d'impact relative à la protection des données

Lorsque le CSCSP envisage un traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes, une analyse d'impact (AIPD) est effectuée avant la mise en œuvre. L'AIPD est conduite sous la responsabilité de la Conseillère ou du Conseiller à la protection des données, qui en conserve la documentation et rend compte à la Direction.

Art. 21 – Gestion des incidents et violations de sécurité

1 Le service informatique et la Conseillère ou le Conseiller à la protection des données examinent toute violation de la sécurité des données personnelles et proposent les mesures correctives nécessaires.

2 Le CSCSP informe le PFPDT dans les plus brefs délais et, le cas échéant, les personnes concernées, si la violation présente un risque élevé pour les droits de celles-ci.

Art. 22 – Utilisation des outils numériques et de l'intelligence artificielle

L'utilisation des outils informatiques et de l'intelligence artificielle (IA) au sein du CSCSP font l'objet de directives spécifiques auxquelles il est expressément renvoyé[8].

Art. 23 – Externalisation du traitement des données

Le CSCSP peut confier certaines activités de traitement à des prestataires externes (hébergement, formation, analyse statistique, etc.) lorsque cela est justifié par son organisation ou sa mission. Le contrat écrit précise les obligations du prestataire telles qu'elles découlent de l'art. 11 du présent règlement.

7 Communication, transparence et transfert de données

Art. 24 – Destinataires internes

Les données personnelles doivent être communiquées uniquement aux personnes dûment autorisées selon le principe du besoin d'en connaître.

Art. 25 – Destinataires externes

1 Le CSCSP ne communique les données personnelles à des destinataires externes que lorsque cela est prévu par la loi ; nécessaire à l'exécution d'un contrat ou d'un mandat confié par le CSCSP, ou si la personne concernée a donné son consentement explicite.

2 Les données peuvent être transmises, notamment aux autorités fédérales (SEFRI, OFJ, OFS, OFSP, etc.) ou cantonales (par exemple : les établissements pénitentiaires), aux institutions partenaires dans le domaine de la formation, de la recherche ou de la politique d'exécution des mesures et sanctions pénales ou de la probation, prestataires techniques et sous-traitants. Ceux-ci doivent fournir des garanties de sécurité suffisantes.

Art. 26 – Communication à l'étranger

En principe, le CSCSP ne communique pas de données personnelles à l'étranger, cas échéant, les dispositions de la LPD s'appliquent.

Art. 27 – Communication aux médias

La personne en charge de traiter des données qui communique des données à des autorités, médias ou tiers, doit strictement respecter le secret de fonction, la confidentialité et la protection des intérêts du CSCSP. Ces communications doivent être validée par la Direction, la responsable de la communication ou la Conseillère ou le Conseiller à la protection des données, documentées de manière à garantir la traçabilité et la conformité à la LPD.

[8] Voir : Directive sur l'usage des technologies de l'IA

8 Contrôle, surveillance et dispositions finales

Art. 28 – Autorité de surveillance

1 Le CSCSP est soumis, à la Loi fédérale sur la protection des données et à la surveillance du Préposé fédéral à la protection des données et à la transparence (PFPDT).

2 Le CSCSP collabore pleinement avec le PFPDT et lui fournit toute information nécessaire à l'exercice de ses compétences.

Art. 29 – Contrôle interne et audit

Sur mandat de la Direction, la Conseillère ou le Conseiller à la protection des données effectue des vérifications régulières sur la conformité des traitements, formule des recommandations ou des mesures correctives, et consigne l'ensemble dans le registre interne de conformité.

Art. 30 – Soumission et approbation du règlement

1 Le CSCSP communique le présent règlement au Préposé fédéral à la protection des données et à la transparence pour information.

2 En cas de modifications substantielles ou de nouveaux traitements présentant un risque élevé pour les droits et libertés des personnes concernées, le CSCSP consulte le PFPDT avant leur adoption.

3 Le règlement entre en vigueur après validation par le Conseil de fondation du CSCSP le 4 décembre 2025.

Art. 31 – Violations et sanctions internes

1 En cas de non-respect du présent règlement, la Direction peut prononcer des mesures disciplinaires contre la collaboratrice ou le collaborateur concerné·e, conformément aux règles internes applicables.

2 En présence de violations graves tombant sous le coup du droit pénal, le CSCSP se réserve le droit d'informer les autorités judiciaires compétentes.

3 En cas de violation du règlement par les sous-traitants et partenaires externes, le CSCSP pourra résilier le contrat et se retourner contre le sous-traitant ou le partenaire externe.

Art. 32 – Réparation du dommage et du tort moral

1 Toute personne ayant subi un dommage ou une atteinte à sa personnalité résultant d'un traitement illicite de ses données a droit à la réparation.

2 La Direction, en coordination avec la Conseillère ou le Conseiller à la protection des données examine toute demande de réparation avec diligence.

3 Le cas échéant, les voies judiciaires prévues par la législation fédérale demeurent réservées.

Art. 33 – Évaluation et mise à jour

1 Le règlement fait l'objet d'une évaluation périodique, au minimum tous les trois ans, ou en cas de modification législative ou organisationnelle majeure.

2 Les propositions d'adaptation sont formulées par la Conseillère ou le Conseiller à la protection des données et soumises à la Direction pour approbation.

3 Toute version mise à jour est communiquée à l'ensemble des collaboratrices et collaborateurs.

Art. 34 – Entrée en vigueur

1 Le présent règlement entre en vigueur à la date fixée par le Conseil de fondation du CSCSP et est contraignant pour l'ensemble du personnel du CSCSP.

2 Il abroge et remplace toutes dispositions antérieures contraires en matière de protection des données.

Le texte de référence est conservé dans les archives officielles du CSCSP.

Fribourg, le 1er janvier 2026

Le Président du Conseil de Fondation CSCSP,

Andreas Michel