Titre abrégé
Règlement de la CRS Canton de Berne sur la protection des données
Objectif et finalité
Le présent règlement fixe des règles contraignantes pour le traitement des données personnelles au sein de la CRS Canton de Berne. Ces prescriptions impératives internes constituent, en sus des règlements, la base et la garantie de la protection des données personnelles.
Champ d'application
Le présent règlement s'applique aux collaborateurs/-trices, aux personnes investies d'une charge honorifique et aux bénévoles de la CRS Canton de Berne, ainsi qu'aux personnes mandatées par la CRS Canton de Berne, sur tous les sites, en Suisse et à l'étranger.

SRK Kanton Bern
Bernstrasse 162
Postfach
3052 Zollikofen
Telefon 031 919 09 09
kvbe@srk-bern.ch
www.srk-bern.ch

Table des matières

1. Introduction

Du fait de ses nombreuses activités, la Croix-Rouge suisse Canton de Berne (CRS Canton de Berne) collecte et traite un volume considérable de données personnelles. Les sept Principes fondamentaux de la Croix-Rouge, qui guident notre travail au quotidien, nous engagent à accorder toute l'attention requise à la protection de ces données, et notamment aux données sensibles. Nous préservons le droit individuel des personnes concernées à la protection de leur vie privée et de leur personnalité. Les prescriptions relatives à la protection des données s'appliquent chaque fois que des données personnelles font l'objet d'une activité de traitement.

Les principes de la CRS en matière de protection des données adoptés par le Conseil de la Croix-Rouge définissent le cadre et l'importance de la gestion des données personnelles au sein de la CRS Canton de Berne. Le présent règlement fixe des règles contraignantes pour le traitement des données personnelles et peut être complété par d'autres directives d'exécution spécifiques aux différents domaines.

Le présent règlement entend mettre à la disposition des collaborateurs/-trices, des personnes investies d'une charge honorifique et des bénévoles de la CRS Canton de Berne en Suisse et à l'étranger un guide et un manuel. Les directives et processus auxquels elle se réfère doivent être suivis. Toute précision à ce sujet peut être obtenue auprès du / de la conseiller/-ère à la protection des données (datenschutz@srk-bern.ch).

Les collaborateurs/-trices, les personnes investies d'une charge honorifique et les bénévoles de la CRS Canton de Berne sont tenus de se conformer aux dispositions du présent règlement et des directives d'exécution. Le respect des prescriptions est régulièrement contrôlé. En cas de manquement ou d'abus, les mesures requises sont prises. Il incombe aux propriétaires des données de motiver et de consigner par écrit toute dérogation ou exception au présent règlement qui se révèlerait nécessaire.

Lien du présent règlement avec les dispositions légales applicables : La CRS Canton de Berne est soumise aux dispositions de la loi fédérale sur la protection des données (LPD) et de l'ordonnance connexe. Dans le cadre des offres fournies à des personnes physiques au sein de l'Union européenne (UE) ou de l'Espace économique européen (EEE), ou de l'observation du comportement de ces personnes, les dispositions européennes prévues par le règlement général sur la protection des données (RGPD) lui sont également applicables. Le présent règlement aborde dans le détail les dispositions légales pertinentes. Si l'une de ses dispositions devait conduire à une violation de la LPD ou du RGPD, il conviendrait d'en informer le/la conseiller/-ère à la protection des données.

2. Responsabilités

2.1 Responsabilités au sein de la CRS Canton de Berne

S'agissant du respect et de la mise en œuvre de la protection des données, les responsabilités au sein du Siège de la CRS Canton de Berne sont définies comme suit :

- Le **Conseil de la Croix-Rouge** approuve les principes de la CRS en matière de protection des données, lesquels s'appliquent dans toutes les organisations et au Siège de la CRS en sus des dispositions légales.

- Le **Comité de direction de la CRS Canton de Berne** approuve le règlement de la CRS Canton de Berne sur la protection des données et endosse la responsabilité stratégique de la protection du traitement des données personnelles.

- Le/la **directeur/-trice et la direction** veillent à leur mise en œuvre, acceptent et assument le risque opérationnel.

- Le/la **responsable informatique de la CRS Canton de Berne**, en tant que préposé-e à la sécurité de l'information est responsable de la sécurité des informations et des données, ainsi que de la sécurité physique, technique et organisationnelle. Il/elle fournit ainsi une contribution importante au respect des dispositions sur la protection des données.

- Le **Service juridique du Siège de la CRS,** le/la **conseiller/-ère en protection des données du Siège de la CRS** ou le/la **responsable de la sécurité de l'information du Siège de la CRS** ont compétence pour clarifier toutes les questions juridiques en rapport avec la protection des données personnelles ou des informations. Il procède à un contrôle préalable de tous les contrats afin de s'assurer qu'ils sont conformes au droit en vigueur dans ce domaine.

- Les **propriétaires des données** sont responsables d'une collecte de données ou d'une activité de traitement. Il leur incombe de veiller à la protection et à la classification en bonne et due forme des données personnelles et des informations. Ils prennent les décisions relatives à l'accès aux données, à leur modification et à leur transmission et engagent des mesures appropriées afin de prévenir les accès non autorisés.

- Les **collaborateurs/-trices,** les **personnes investies d'une charge honorifique,** les **bénévoles** et les **personnes mandatées** par la CRS Canton de Berne répondent de la protection des données dans leur domaine d'activité. Il est attendu qu'ils fassent preuve d'esprit critique et adoptent un comportement responsable. Dans ce but, ils bénéficient de mesures de sensibilisation et de formation adaptées à leurs fonctions respectives.

- Les **chef-fe-s de département et de service** sont tenus de garantir le respect des prescriptions du présent règlement par des mesures organisationnelles, personnelles et techniques, et de veiller à ce que les responsables du traitement de données se conforment à leurs obligations.

Les infractions à la LPD peuvent entraîner de fortes amendes pour les collaborateurs/-trices, les personnes investies d'une charge honorifique et les bénévoles qui traitent concrètement des données personnelles. En tant qu'employeur, la CRS Canton de Berne peut en outre prononcer des sanctions allant jusqu'à la résiliation immédiate des rapports de travail.

2.2 Conseiller/-ère à la protection des données

Le/la conseiller/-ère à la protection des données conseille la CRS Canton de Berne, les départements et les services en la matière. Le terme de « conseiller/-ère à la protection des données » défini dans la LPD est utilisé au sein de la CRS Canton de Berne de manière analogue au terme « préposé-e à la protection des données ». Il correspond à l'appellation anglaise « *Data Protection Officer* » (DPO).

Le/la conseiller/-ère à la protection des données est l'interlocuteur/-trice des personnes concernées, du Préposé fédéral à la protection des données et à la transparence (PFPDT) et des autorités chargées de la protection des données en Suisse. La CRS Canton de Berne publie ses coordonnées sur Internet et les communique au PFPDT.

Le/la conseiller/-ère à la protection des données est consulté-e en amont des nouveaux projets, ainsi que des futures collaborations avec des prestataires externes. En cas de divergence d'opinions, le/la directeur/-trice tranche après avoir procédé à une pesée des intérêts.

Le/la conseiller/-ère à la protection des données concourt à l'application des dispositions relatives à la protection des données, notamment en examinant le traitement des données personnelles et en recommandant à la direction des mesures lorsqu'il/elle constate une violation des prescriptions de

protection. La CRS Canton de Berne veille à ce qu'il/elle soit informé-e de toute violation de la sécurité des données.

Le/la conseiller/-ère à la protection des données conseille la CRS Canton de Berne dans l'élaboration des analyses d'impact relatives à la protection des données et contrôle leur exécution dans le cadre des activités de la CRS Canton de Berne en tant qu'organe fédéral. Il/elle informe sur la mise en œuvre et les aspects de la protection des données dans des notices et sur le portail thématique de l'intranet de la CRS Canton de Berne. Il/elle forme et conseille le personnel de la CRS Canton de Berne dans le domaine de la protection des données.

Le/la conseiller/-ère à la protection des données exerce sa fonction de manière indépendante par rapport à la CRS Canton de Berne et sans recevoir d'instruction de celle-ci. Dans les cas importants, il/elle a le droit d'informer le/la directeur/-trice de la CRS Canton de Berne.

La CRS Canton de Berne met les ressources nécessaires à la disposition du / de la conseiller/-ère à la protection des données et lui donne accès à tous les renseignements, documents, registres des activités de traitement et à toutes les données personnelles dont il/elle a besoin pour l'accomplissement de ses tâches.

3. Principes généraux en matière de traitement de données personnelles

Tous les collaborateurs/-trices, les personnes investies d'une charge honorifique et les bénévoles respectent les principes généraux définis dans la LPD. Sont également applicables les principes de la CRS en matière de protection des données approuvés par le Conseil de la Croix-Rouge.

Les collaborateurs/-trices responsables du traitement (propriétaires des données) doivent être en mesure de prouver pour chaque traitement de données personnelles que les principes ci-dessous ont été suivis.

Principe	Description
Licéité	Tout traitement de données personnelles doit être licite. Si une base légale est requise, les données ne peuvent être traitées que si et dans la mesure où elle existe pour chacune des opérations de traitement envisagées (cf. chapitre 4).
Transparence, bonne foi	Traiter les données en toute bonne foi exige une gestion des données honnête, équitable, responsable et licite. Les personnes concernées sont informées de manière précise et compréhensible sur le/la responsable des données, la finalité du traitement, les possibles (catégories de) destinataires des données, les liens avec l'étranger et, en cas de collecte de données indirecte, sur le type de données (cf. chapitre 5).
Utilisation dans un but déterminé	Les données personnelles doivent être collectées et traitées pour des finalités déterminées et reconnaissables pour la personne concernée, et uniquement d'une manière compatible avec ces finalités.
Proportionnalité	Seules peuvent être collectées et traitées les données personnelles absolument nécessaires à l'accomplissement des tâches ou à la réalisation de la finalité du traitement et qui sont appropriées à cet effet. Sauf délais d'archivage ou de conservation à respecter, ou sauf existence d'un intérêt à leur conservation, les données personnelles qui ne sont plus nécessaires doivent être détruites ou anonymisées dans les meilleurs délais.
Exactitude des données	Les données personnelles traitées doivent être exactes et tenues à jour. Toutes les mesures appropriées doivent être prises afin de le garantir.

Sécurité et confidentialité	Les données personnelles doivent être protégées pendant tout le processus de traitement et de conservation. Elles doivent être sécurisées par des mesures appropriées (cf. chapitre 8) et traitées de manière confidentielle.
Protection des données dès la conception et par défaut	Dès le début de leur conception, les systèmes doivent être développés et configurés de façon à garantir la protection des données (privacy by design), et leurs paramétrages par défaut doivent toujours offrir la meilleure protection possible des données (privacy by default).

4. Licéité du traitement des données personnelles

Le traitement de données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées. Le traitement et la collecte de données personnelles ne sont pas illicites quand il existe un motif justificatif du fait du consentement de la personne concernée, d'un intérêt privé ou public prépondérant, ou de la loi.

On distingue les motifs justificatifs suivants :

- Consentement de la personne concernée
- Exécution d'un contrat
- Intérêt privé ou public prépondérant
- Base légale
- Recherche, planification ou statistique

Préalablement à tout nouveau traitement de données, le/la propriétaire des données doit s'assurer (au besoin avec l'appui du / de la conseiller/-ère à la protection des données) qu'il existe, le cas échéant, un motif justificatif (cf. chapitre 7). Les différents motifs justificatifs et les cas particuliers sont précisés et illustrés dans les paragraphes qui suivent.

4.1 Consentement de la personne concernée

Le consentement de la personne concernée est un motif justificatif très actif et transparent.

Avant de donner son consentement, la personne concernée doit être pleinement informée sur l'identité du / de la responsable des données, la finalité du traitement, les possibles (catégories de) destinataires des données, les liens avec l'étranger et, en cas de collecte de données indirecte, sur le type de données (cf. chapitre 5.1). Le consentement n'est lié à aucune exigence formelle, mais doit être donné librement et indubitablement. Pour des raisons de preuve, une déclaration écrite ou électronique est recommandée.

Un consentement exprès est requis pour le traitement de **données personnelles sensibles** et pour le **profilage à haut risque** (cf. définitions en annexe). Il peut être donné par écrit (format papier ou électronique), mais aussi oralement, étant entendu qu'il y a lieu de privilégier une déclaration susceptible d'être prouvée. De même, le consentement peut être exprimé valablement au moyen d'une case à cocher ou d'un clic sur un bouton en ligne (p. ex. le bouton « Continuer »). Un consentement en blanc n'est pas admissible. Il ne saurait y avoir consentement lorsqu'aucune action n'est requise de la part de la personne concernée.

4.2 Exécution d'un contrat

Les données personnelles de bénéficiaires de prestations, de client-e-s ou de cocontractant-e-s peuvent être collectées et traitées sans consentement aux fins de conclure, d'exécuter et de résilier un contrat. Le traitement des données comprend aussi la gestion des relations avec ces personnes, pour autant que celle-ci soit liée à l'objet du contrat (p. ex. remerciements à la suite d'un don). En l'absence d'un tel lien, c'est-à-dire lorsqu'on entend traiter les données dans un autre but (p. ex. pour adresser

des appels aux dons aux bénéficiaires d'une prestation), un motif justificatif est requis – en priorité sous la forme du consentement de la personne concernée, laquelle doit être préalablement informée en toute transparence.

4.3 Intérêt privé ou public prépondérant

La CRS Canton de Berne doit pouvoir collecter et traiter des données personnelles afin d'accomplir son mandat. Dans ce contexte, elle est autorisée à traiter des données personnelles pour mener à bien une activité de traitement, même si cela est dans une certaine mesure en contradiction avec les intérêts de la personne concernée (d'où l'intérêt privé « prépondérant » de la CRS Canton de Berne). Un intérêt public est jugé prépondérant lorsque, par exemple, les intérêts vitaux d'une personne sont en jeu, que la sécurité intérieure de la Suisse est menacée ou que des données sont communiquées à l'étranger pour des raisons humanitaires, dans le cadre de la recherche de personnes disparues dans une zone de conflit ou lors d'une catastrophe naturelle.

Cette pesée des intérêts doit toujours être effectuée en concertation avec le/la conseiller/-ère à la protection des données.

4.4 Base légale

La collecte et le traitement de données personnelles sont admis quand ils sont expressément prévus par une loi, une ordonnance ou un autre acte législatif. De nombreuses lois fédérales contiennent des prescriptions spécifiques en matière de protection des données, par exemple en ce qui concerne la reconnaissance des diplômes étrangers, l'obtention d'un extrait du casier judiciaire ou du registre des poursuites, l'examen du droit aux assurances sociales, les inscriptions dans des registres de personnes, etc. En pareil cas, il n'y a pas lieu en principe de solliciter le consentement de la personne concernée, puisque le traitement des données est autorisé en vertu de prescriptions légales. Pour une interprétation sans équivoque de la base légale, il convient de faire appel au / à la conseiller/-ère à la protection des données.

4.5 Recherche, planification ou statistique

Ce dernier motif justificatif implique que les données personnelles sont traitées uniquement à des fins ne se rapportant pas à des personnes, dans le cadre de la recherche, de la planification ou de la statistique. Différentes conditions doivent être réunies. Tout d'abord, les données doivent être anonymisées dès que la finalité du traitement le permet. Si une anonymisation est impossible ou exige des efforts disproportionnés, des mesures appropriées doivent être prises afin que les personnes concernées ne puissent pas être identifiées. S'il s'agit de données sensibles, elles ne peuvent être communiquées à des tiers que sous une forme ne permettant pas d'identifier les personnes concernées ; si cela n'est pas possible, des mesures doivent être prises qui garantissent que les tiers ne traitent les données qu'à des fins ne se rapportant pas à des personnes. Les résultats sont publiés sous une forme ne permettant pas d'identifier les personnes concernées.

5. Droits de la personne concernée

Dans ses principes en matière de protection des données, la CRS Canton de Berne s'engage à préserver le droit des personnes concernées à obtenir des informations complètes sur les données personnelles qu'elle stocke, ainsi que leur droit d'accès, leur droit de rectification, leur droit à l'effacement et leur droit à la portabilité de ces données. Aussi la CRS Canton de Berne a-t-elle mis en place des processus qui garantissent intégralement les droits des personnes concernées dans le respect des délais prescrits.

5.1 Droit à des informations transparentes et complètes

En vertu du principe de transparence, la personne concernée a droit à des informations complètes, que le responsable du traitement[1] (cf. définitions en annexe) a l'obligation de lui fournir. Sans ces renseignements, la personne concernée ne peut pas savoir que ses données personnelles sont traitées, ni comment elles le sont, et ne peut donc pas faire valoir les droits qui lui sont garantis par la loi.

La personne concernée doit être informée au moins de l'identité du responsable du traitement, de la finalité du traitement, des (catégories de) destinataires auxquels ses données personnelles sont communiquées (cf. chapitre 6.2), si ces données sont transmises à l'étranger, du nom de l'État ou de l'organisme international concerné (cf. chapitre 6.3), et, si les données n'ont pas été collectées auprès d'elle, des catégories de données traitées. Si les informations sont fournies par des moyens collectifs, tels que la déclaration de protection des données publiée sur le site Web de la CRS Canton de Berne, il convient toujours d'y renvoyer individuellement. Lorsque ses données sont collectées, la personne concernée doit recevoir les principales informations dès le premier niveau de communication.

5.2 Autres droits

Outre le droit à des informations transparentes et complètes, toute personne dont les données personnelles sont traitées de la CRS Canton de Berne peut faire valoir les droits suivants :

- le droit d'obtenir des renseignements (**droit d'accès**), notamment sur l'origine des données personnelles enregistrées la concernant, la finalité de la collecte et de l'utilisation, la durée de conservation prévue, le type de traitement et les tiers à qui les données sont communiquées ;
- le droit de **rectifier** et/ou de **compléter** ses données personnelles pour le cas où celles-ci seraient inexactes ou incomplètes ;
- le droit de **s'opposer** au traitement des données personnelles nécessaires au regard de la finalité ou de le **limiter** ;
- le droit de **révoquer un consentement** ;
- le droit à l'**effacement** des données personnelles, pour autant que des motifs légaux impératifs ou des intérêts prépondérants (justifiés) n'exigent pas leur stockage et leur traitement ultérieur. Le cas échéant, l'effacement peut également consister à anonymiser les données ;
- le droit à la **portabilité des données**, c'est-à-dire à la remise ou à la transmission, sous un format électronique, des données personnelles que la CRS Canton de Berne traite de manière automatisée avec le consentement de la personne concernée, ou en relation directe avec la conclusion ou l'exécution d'un contrat conclu entre la CRS Canton de Berne en tant que responsable du traitement et la personne concernée ;
- le droit d'introduire une **réclamation** auprès de l'autorité de surveillance compétente en cas de violation des prescriptions de protection des données.

La mise en œuvre précise de ces droits ainsi que les procédures y relatives sont réglées dans la LPD.

6. Communication de données personnelles à des tiers

Dans certains cas, les données personnelles sont non seulement traitées de la CRS Canton de Berne, mais aussi communiquées à des tiers pour des raisons précises – par exemple à des partenaires contractuels, à des organisations de la Croix-Rouge ou à des autorités. Afin que cette communication soit licite, elle requiert un motif justificatif, en particulier si les données personnelles sont traitées à d'autres fins ou que des données sensibles sont communiquées (cf. chapitre 4).

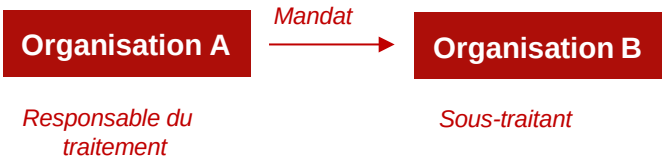
[1] Les termes « responsable », ainsi que « sous-traitant » et « destinataire » étant des concepts légaux renvoyant principalement à des personnes morales, seule la forme masculine est utilisée ici.

6.1 Communication à des destinataires internes (au sein de la CRS Canton de Berne)

En principe, les données personnelles peuvent être transmises à des destinataires internes, c'est-à-dire à d'autres départements ou services de la CRS Canton de Berne, si l'accomplissement du mandat l'exige.

6.2 Communication à des destinataires externes

Lorsqu'un tiers traite des données personnelles pour le compte et sur instruction de la CRS Canton de Berne sans en avoir reçu l'entière responsabilité, on parle de **sous-traitance**. La sous-traitance n'est autorisée que si elle est légalement ou contractuellement possible (p. ex. si elle n'est pas interdite par le secret médical ou par une clause de confidentialité stipulée dans un contrat) et si le sous-traitant effectue le traitement comme l'effectuerait le responsable du traitement lui-même. La transmission de données personnelles au sein de la même personne morale (cf. chapitre 6.1) ne constitue pas une sous-traitance.



Exemples :

- L'organisation A charge l'organisation B d'imprimer et d'expédier des appels aux dons. À cet effet, elle lui donne accès à sa base de données des donateurs/-trices.
- L'organisation A stocke ses documents sur les serveurs de l'organisation B.

En cas de sous-traitance, **le responsable du traitement** s'acquitte des trois obligations suivantes :

- Sélection rigoureuse : Le sous-traitant doit être sélectionné avec soin. Le responsable du traitement doit s'assurer qu'il est en mesure de répondre aux exigences légales en matière de protection et de sécurité des données.

- Instructions rigoureuses : Toutes les instructions nécessaires à l'accomplissement des tâches doivent faire l'objet d'un contrat avec le sous-traitant. Plus le risque lié au traitement est élevé, plus le responsable du traitement doit être attentif à la formulation de ses instructions.

- Surveillance rigoureuse : Afin de prévenir tout manquement, le responsable du traitement est tenu de s'assurer que le sous-traitant respecte les obligations découlant du droit relatif à la protection des données ainsi que le mandat convenu contractuellement.

Si le sous-traitant se trouve à l'étranger, le responsable du traitement doit en outre tenir compte des dispositions du chapitre 6.3. En vertu des principes de la CRS en matière de protection des données, les données personnelles sont, dans la mesure du possible, stockées uniquement en Suisse et dans l'UE.

Le sous-traitant est tenu de respecter les obligations légales et contractuelles qui lui incombent – en particulier, il n'est autorisé à traiter les données personnelles que conformément aux instructions du responsable du traitement. Il peut faire valoir les mêmes motifs justificatifs que le responsable du traitement. Le sous-traitant peut lui-même sous-traiter un traitement à un tiers (sous-traitant ultérieur) à condition d'y avoir été autorisé par le responsable du traitement.

En cas de violation de la sécurité des données, le sous-traitant est tenu d'informer sans retard le responsable du traitement afin qu'il puisse décider des suites à donner.
Du fait de ses nombreuses activités, la CRS Canton de Berne est à la fois responsable du traitement et sous-traitant. Ces rôles sont à définir contractuellement au cas par cas, dans le cadre de **contrats de sous-traitance de données personnelles.** Chacun de ces contrats doit spécifier l'ensemble des tâches confiées au sous-traitant par le responsable du traitement, ainsi que les obligations et les responsabilités de chacune des parties. Tous les contrats sont vérifiés avant d'être signés et classés de manière centralisée.

6.3 Communication de données personnelles à l'étranger ou à des organismes internationaux

La communication de données personnelles à l'étranger (c'est-à-dire en dehors de Suisse) ou à des organismes internationaux (p. ex. le CICR) est en principe possible dès lors que le pays destinataire dispose d'un niveau de protection des données adéquat.

Le Conseil fédéral tient à l'annexe 1 de l'ordonnance sur la protection des données une liste des États indiquant le niveau de protection garanti.

Lorsque le niveau de protection garanti *n'est pas* adéquat, la communication de données personnelles à l'étranger est néanmoins possible à certaines conditions, par exemple :

- quand la personne concernée a expressément donné son consentement à la communication de ses données à l'étranger ;
- quand la communication des données à l'étranger est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers et qu'il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable ;
- quand la communication des données à l'étranger est en relation directe avec la conclusion ou l'exécution d'un contrat.

La transmission de données à l'étranger est traitée à part dans une directive spécifique ou une notice.

7. Registre et documentation des activités de traitement

La CRS Canton de Berne a l'obligation légale de tenir un registre de ses activités de traitement et de conserver la preuve de la conformité de ces dernières à la législation sur la protection des données. En conséquence, toute nouvelle activité de traitement doit faire l'objet d'un examen préalable, puis être documentée dans le répertoire central[2]. Cette obligation vise essentiellement à améliorer la transparence au sein de l'organisation et à assurer ainsi une meilleure protection des données personnelles.

Les collaborateurs/-trices de la CRS Canton de Berne sont progressivement informés de ces obligations ainsi que formés. Les informations pertinentes sur la protection des données sont accessibles à tous via l'accès au dépôt central.

7.1 Registre des activités de traitement

Ce registre consiste en une description générale des activités de traitement. Les principaux contenus du répertoire en tant que responsable sont : la finalité du traitement, les catégories de personnes concernées et de données personnelles, les destinataires internes et externes, les références à l'étranger, la durée de conservation ainsi que les mesures de sécurité des données.

[2] Par répertoire central, on entend Scodi 4P, Intranet, etc.

Tant le responsable du traitement que le sous-traitant doivent tenir un registre des activités de traitement, qui est déposé dans le Scodi 4P.

Les propriétaires des données (cf. chapitre 2) répondent de la vérification régulière et de la documentation des nouveaux traitements de données.

7.2 Nouvelles activités de traitement

Les propriétaires des données ont l'obligation d'annoncer au/à la conseiller/-ère à la protection des données les activités de traitement nouvelles ou modifiées afin qu'elles puissent être contrôlées au préalable et mises à jour dans le registre des activités de traitemedirect. Lors de la planification de nouveaux travaux (projets, applications, processus, etc.), le/la conseiller/-ère à la protection des données et le/la préposé-e à la sécurité de l'information doivent être impliqués dès que possible pour permettre la prise en compte des mesures nécessaires (protection des données dès la conception et par défaut). Au besoin, ils/elles définissent des mesures appropriées en concertation avec les propriétaires des données. Ils/elles vérifient également les nouvelles activités de traitement saisies le registre central, notamment quant à leur conformité au présent règlement et aux dispositions légales, à la nécessité d'une analyse d'impact sur la protection des données ou de mesures garantissant la sécurité, ainsi qu'à d'éventuels accords contractuels.

Exemples de nouvelles activités de traitement : collecte de numéros de passeport pour l'organisation de voyages, introduction de Google Analytics, acquisition d'une application pour la gestion numérique des patient-e-s, externalisation du centre d'appel.

7.3 Analyse d'impact relative à la protection des données personnelles

L'analyse d'impact relative à la protection des données personnelles (AIPD) est un outil qui permet d'identifier et d'évaluer précocement les risques inhérents aux activités de traitement. En cas de besoin, elle sert à définir des mesures appropriées dans le but de réduire les risques pour la personnalité ou les droits fondamentaux de la personne concernée.

Une analyse d'impact relative à la protection des données personnelles doit être effectuée lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. L'existence d'un risque élevé, en particulier lors du recours à de nouvelles technologies, dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Un tel risque existe notamment dans les cas suivants :

- traitement de données sensibles à grande échelle ;
- surveillance systématique de grandes parties du domaine public.

L'AIPD est élaborée par le/la propriétaire des données puis soumise à l'examen du / de la préposé-e à la protection des données. Elle contient une mise en balance des intérêts du responsable du traitement et de ceux de la personne concernée effectuée selon une démarche documentée.

S'il ressort de l'AIPD que, malgré les mesures prévues par la CRS Canton de Bern, le traitement envisagé demeure susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, il y a lieu de consulter le/la conseiller/-ère à la protection des données. Celui-ci/celle-ci ou le/la directeur/-trice est autorisé-e à consulter le PFPDT lorsque cela apparaît nécessaire au regard du résultat de la consultation ou des circonstances.

8. Sécurité des données

Les données personnelles doivent être traitées confidentiellement et d'une manière propre à garantir un niveau de sécurité approprié. Il convient en particulier de les protéger contre tout traitement non autorisé ou illicite ainsi que contre toute perte, destruction ou altération accidentelle.

Afin de garantir un niveau de sécurité adéquat, il convient d'établir le besoin de protection des données personnelles et de déterminer les mesures techniques et organisationnelles appropriées. Les mesures techniques sont directement liées au système informatique et/ou à l'application, lesquels doivent remplir certains critères pour pouvoir garantir la sécurité des données personnelles. Les mesures organisationnelles concernent l'environnement du système informatique, notamment les personnes qui l'utilisent et leur entourage. Seule l'association de ces deux types de mesures est à même de prévenir la destruction ou la perte de données, ou encore les erreurs, les falsifications et les accès non autorisés.

Les principales mesures techniques et organisationnelles sont les suivantes :

- pseudonymiser et crypter les données conservées et échangées,
- assurer la confidentialité, l'intégrité et la disponibilité des applications,
- journaliser les opérations de traitement et, dans certains cas, conserver les procès-verbaux séparément du système dans lequel les données personnelles sont traitées,
- répartir et séparer soigneusement les rôles et les compétences selon le principe du « besoin d'en connaître »,
- protéger la vie privée dès la conception du système et par défaut,
- contrôler et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles qui ont été prises.

Les mesures techniques et organisationnelles doivent être adaptées à l'état de la technique, à la nature et à l'étendue du traitement de données, ainsi qu'aux risques de ce dernier pour la personnalité et les droits fondamentaux des personnes concernées. Plus le risque est grave, plus il est probable et plus le traitement est étendu, et plus les mesures techniques et organisationnelles doivent répondre à des exigences strictes pour être considérées comme appropriées.

Les exigences en matière de sécurité des données sont définies dans les normes juridiques y relatives et les directives sur la sécurité de l'information de la CRS Canton de Berne. Les aspects des directives sur la sécurité de l'information ayant des implications pour la protection des données doivent être élaborés et mis en œuvre après consultation avec le/la conseiller/-ère à la protection des données.

9. Conservation et effacement de données personnelles

Les données personnelles doivent être protégées tout au long de leur cycle de vie, c'est-à-dire depuis leur collecte et leur introduction dans les applications jusqu'à leur destruction, leur anonymisation ou leur archivage, ainsi que durant toutes les étapes du traitement.

9.1 Délais de conservation des données personnelles

Les données personnelles ne peuvent être traitées et conservées plus longtemps qu'il n'est nécessaire pour atteindre le but dans lequel elles ont été collectées. Il est toutefois possible de prolonger la conservation pour les motifs suivants :

- respect d'obligations légales (p. ex. obligations de conservation et de documentation découlant du droit civil ou fiscal) ;
- respect d'obligations contractuelles (p. ex. établissement d'un certificat de travail) ;
- respect d'intérêts privés légitimes (p. ex. faire valoir ou défendre ses droits en justice).

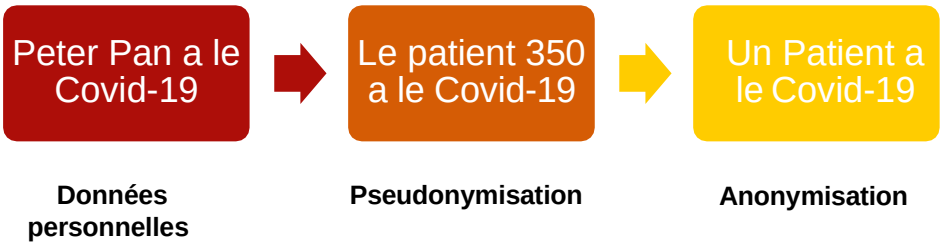
La durée et les délais de conservation ne sont pas toujours faciles à fixer et doivent faire l'objet de décisions au cas par cas. Les exigences formulées dans la directive relative aux délais de conservation constituent la base de référence à cet égard.

9.2 Pseudonymisation et anonymisation de données personnelles

La pseudonymisation et l'anonymisation de données personnelles permettent de faire en sorte que les personnes dont les données sont traitées dans un système ne puissent plus être identifiées.

La **pseudonymisation** consiste à remplacer par des informations neutres (pseudonyme) toutes les informations permettant le rattachement à une personne donnée. Un tableau de concordance indique quel pseudonyme correspond à quelles données d'identification. Tant que ce tableau existe et est accessible, la pseudonymisation est réversible. Les données personnelles pseudonymisées restent des données personnelles soumises aux principes de la protection des données.

L'**anonymisation,** en revanche, consiste à supprimer définitivement les éléments d'identification ainsi que toute possibilité de retrouver les informations d'origine. La personne n'est plus identifiable, et le processus est irréversible. Les données complètement anonymisées ne sont donc plus considérées comme des données personnelles.



Si la pseudonymisation est considérée comme une mesure utile pour accroître la protection des données, l'anonymisation est une solution alternative à l'effacement des données personnelles. Il convient de recourir à ces deux procédés aussi souvent que possible.

9.3 Effacement de données personnelles

Dès que les données personnelles ne sont plus nécessaires au regard de la finalité du traitement, elles doivent être détruites ou rendues anonymes. Il en va de même lorsqu'une personne concernée demande expressément l'effacement de ses données. S'agissant des données stockées sur un support électronique, un simple effacement est souvent insuffisant, et il convient de les supprimer de telle sorte qu'elles soient définitivement inaccessibles. Quant aux données personnelles sur papier, en particulier les données personnelles sensibles, elles doivent être passées à la broyeuse. Les supports de données et les médias relèvent de la directive relative à la sécurité en matière d'effacement et/ou de destruction d'informations.

10. Annonce d’une violation de la protection des données

On entend par « violation de la protection des données » (data breach) toute atteinte interne ou externe à la sécurité de données personnelles qui entraîne

- la destruction,
- la perte,
- l’altération,
- l’accès non autorisé, ou
- l’utilisation illicite

de ces données et qui risque ainsi de compromettre gravement les intérêts et les droits des personnes concernées.

10.1 Annonce au sein de la CRS Canton de Berne

Les collaborateurs/-trices, les personnes investies d’une charge honorifique et les bénévoles de la CRS Canton de Berne doivent annoncer sans retard au / à la préposé-e à la sécurité de l’information et au / à la conseiller/-ère à la protection des données tout incident qui s’est produit ou risque de se produire. La règle est la même lorsqu’un sous-traitant annonce à la CRS Canton de Berne un cas de violation de la protection des données.

Le/la conseiller/-ère à la protection des données, appuyé-e par les services pertinents, examine l’incident sous l’angle d’une éventuelle violation de la protection des données, et recommande des mesures afin d’atténuer autant que possible les conséquences pour la personne concernée et la CRS. Ces mesures sont mises en œuvre par tous les services pertinents (service concerné, Service juridique, Communication, Informatique, Développement technique, etc.). Si nécessaire, la violation est annoncée aux autorités de surveillance compétentes (en premier lieu le PFPDT) et aux personnes concernées.

10.2 Annonce au PFPDT

Tout cas de violation de la sécurité des données personnelles pouvant entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée doit être annoncé au PFPDT dans les meilleurs délais à compter du moment où l’on a connaissance du traitement (présumé) non autorisé.

L’annonce doit comprendre toutes les informations nécessaires pour clarifier la situation, en particulier :

- la nature de la violation de la protection des données;
- dans la mesure du possible, le moment et la durée ;
- dans la mesure du possible, les catégories et le nombre approximatif de données personnelles concernées ;
- dans la mesure du possible, les catégories et le nombre approximatif de personnes concernées ;
- les conséquences, y compris les risques éventuels, pour les personnes concernées ;
- les mesures prises ou prévues pour remédier à la situation et atténuer ses conséquences.

L’annonce incombe au / à la conseiller/-ère à la protection des données, d’entente avec le/la directeur/-trice.

10.3 Annonce aux personnes concernées

La personne concernée doit être informée de la violation de ses données personnelles lorsque cela est nécessaire à sa protection, notamment quand elle peut prendre les dispositions nécessaires pour se protéger (modifier son mot de passe p. ex.). La règle est la même lorsque l'annonce est exigée par le PFPDT.

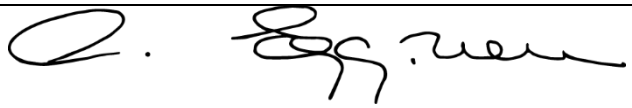
Il est possible de restreindre l'information de la personne concernée, de la différer ou d'y renoncer dans les cas suivants :

- intérêts prépondérants d'un tiers ;
- obligation légale de garder le secret ;
- obligation d'information impossible à remplir ou exigeant des efforts disproportionnés ;
- information d'un grand nombre de personnes au moyen d'une communication publique.

L'annonce incombe au / à la conseiller/-ère à la protection des données, d'entente avec le/la directeur/-trice.

11. Dispositions finales

Le présent règlement est régulièrement révisé et, si nécessaire, adapté. Les collaborateurs/-trices, les personnes investies d'une charge honorifique et les bénévoles sont informés de ces modifications de manière appropriée. L'ensemble de la documentation – règlements, directives, notices, modèles, listes, etc. – est accessible dans le répertoire central.

Valable à partir du :	**Mars 2025**
Signature :	 Présidente, Annalise Eggimann
Date :	28.3.2025
Distribution :	Collaborateurs/-trices, personnes investies d'une charge honorifique et bénévoles de la CRS Canton de Berne
Autorité responsable du document :	Sylwia Galka, conseillère à la protection des données de la CRS Canton de Berne

Annexe : définitions

Terme	Définition
Données personnelles	Toutes les informations concernant une personne physique *identifiée ou identifiable* (ci-après « personne concernée »). Une personne physique est **identifiée ou identifiable** lorsqu'elle peut être identifiée directement ou indirectement. L'identification d'une personne physique peut être réalisée à partir d'une seule information (numéro de téléphone, numéro de maison, numéro AVS, empreintes digitales) ou du croisement d'un ensemble d'informations (adresse, date de naissance, état civil). Elle peut également résulter d'informations déduites des circonstances ou du contexte (identifiant, données de géolocalisation). À la différence des données pseudonymisées, les données anonymisées ne sont plus considérées comme des données personnelles (cf. chapitre 9.2).
Données personnelles sensibles (données sensibles)	Données personnelles qui, en raison de leurs spécificités, nécessitent une protection accrue. En vertu de la loi, sont à considérer comme sensibles les données personnelles suivantes : – les données 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.
Personne concernée	Personne physique dont les données personnelles font l'objet d'un traitement. Contrairement aux personnes physiques (particuliers, individus), les personnes morales (entreprises, etc.) ne sont pas concernées par la LPD.
Traitement	Toute opération relative à des données personnelles, quels que soient la nature et le format du traitement (numérique, papier, oral), notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données
Activité de traitement	Activités ou catégories d'activités dans le cadre desquelles des données personnelles sont traitées, en général dans un but commun
Communication	Fait de transmettre des données personnelles ou de les rendre accessibles
Profilage	Toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant son rendement au travail, sa situation économique, sa santé, ses préférences personnelles, ses intérêts, sa fiabilité, son comportement, sa localisation ou ses déplacements
Profilage à haut risque	Tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de sa personnalité

Responsable du traitement	Personne ou organe fédéral qui, seul-e ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles. En présence de plusieurs responsables du traitement, on parle de responsables conjoints.
Sous-traitant	Personne ou organe fédéral qui traite des données personnelles pour le compte du/des responsable-s du traitement
Propriétaire des données	Personne responsable du traitement des données personnelles, p. ex. chef-fe de service, responsable de secteur ou de projet
Tiers	Toute personne physique ou morale, autorité ou entité autre que la personne concernée, le responsable du traitement et le sous-traitant
Destinataire	Personne physique ou morale, autorité, institution ou entité à laquelle des données personnelles sont divulguées, qu'il s'agisse ou non d'un tiers
Organe fédéral	Autorité fédérale, service fédéral ou personne chargée d'une tâche publique de la Confédération
Organisme international	Toute institution internationale, qu'il s'agisse d'une organisation ou d'un tribunal (p. ex. CICR)
Application	Système, matériel ou logiciel au moyen duquel s'effectue le traitement des données
Pseudonymisation	Fait de modifier des données personnelles de telle sorte qu'elles ne puissent être rattachées à une personne déterminée qu'avec le recours à des informations supplémentaires. Afin d'assurer une protection efficace, ces informations supplémentaires doivent être conservées à part.
Anonymisation	Fait de modifier des données personnelles de telle sorte qu'il soit impossible de les rattacher à la personne concernée. Cette méthode est considérée comme une solution alternative pertinente à l'effacement des données personnelles.