CENTRE FOR CYBER SECURITY BELGIUM

Baseline Information Security Guidelines (BSG) avec RGPD

Édition 2019

CENTRUM VOOR

CYBER SECURITY BELGIUM

Wetstraat 18 – Brussels

CHANCELLERY OF THE PRIME MINISTER

.be

Introduction

Aujourd'hui, nul ne doute que les Technologies de l'Information et de la Communication (TIC) jouent un rôle important dans la vie économique et sociale. Le bon fonctionnement des réseaux, des systèmes informatiques et des logiciels revêt une importance capitale pour les institutions publiques, les organisations qui dépendent largement de leur infrastructure TIC et, par conséquent, du personnel qui en assure le bon fonctionnement.

L'objectif du présent document, "Baseline Security Guidelines (BSG)", est de fournir aux administrations publiques des lignes directrices minimales, sous forme de guide, pour toute implémentation ou évaluation d'un plan de sécurité de l'information afin d'aider les responsables de traitement ainsi que les professionnels dans la gestion de l'information (conseillers en sécurité, responsables informatiques, etc.).

Il n'est donc pas dans l'intention de développer une ligne directrice complète et approfondie, car elle existe déjà.

Ce BSG a été élaboré en collaboration avec des experts de différents Services Publiques Fédéraux (SPF) et des experts externes en tenant compte des standards existants en la matière comme l'ISO/IEC 27001, l'ISO/IEC 27002 et l'ISO/IEC 27701. Et naturellement la RGPD (Règlement Général sur la Protection des Données).

S'il existe de nombreux cadres référentiels ("frameworks") concernant la sécurité de l'information, mais l'utilisation de la norme ISO 2700X comme point de départ présente assurément une valeur ajoutée. Une organisation utilisant un autre cadre peut facilement évaluer si les mesures mises en place sont compatibles avec les directives minimales -reprises dans ce document.

Ce document ne contient aucune instruction de mise en œuvre pratique, ni d'information détaillée sur la manière de procéder conformément aux bonnes pratiques proposées. Nous nous référons à cela à des initiatives telles que FISP ("Federal Information Security Policies", BOSA, 2019) ou le guide de référence sur la cybersécurité (CCB).

Il est également important de mentionner que ces lignes directrices et ce cadre pour la sécurité de l'information ne sont pas indépendants des autres processus, car ils font partie intégrante de la gestion d'entreprise dans sa globalité.

Cela signifie que de nombreuses activités décrites ci-dessous, telles que la gestion des risques, la communication, l'audit et le contrôle et l'amélioration continue, peuvent être réutilisées ou intégrées dans des cadres existants.

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Edition 2019

Dans cette version 2019, des informations spécifiques sont fournies pour intégrer les obligations qui découlent du règlement général sur la protection des données (RGPD)[1] et la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, car l'approche BSG pour la mise en œuvre de la sécurité des informations peut également être appliquée à la mise en œuvre à la protection des données à caractère personnel.

Attention:

Le RGPD se concentre entièrement sur la protection des données à caractère personnel qui comporte également un volet juridique qui n'est pas couvert dans ce guide.

Il existe une différence importante entre la couverture de la sécurité de l'information au niveau de l'entreprise et la protection des données dans le RGPD

La sécurité de l'information et la protection des données à caractère personnel reposent sur les mêmes fondements, mais la sécurité de l'information couvre un champ d'application beaucoup plus large dans le contexte de la protection des données.

Une bonne sécurité des informations dans un contexte commercial inclut non seulement des données personnelles, mais également toutes les autres informations commerciales.

[1] GDPR en anglais

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Table des matières

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

0 Info Document

0.1 Historique

Version	Description et changements
1.0	Premier lancement du BSG
2.0	Intégration des obligations liées au RGPD et à la loi du 30 juillet 2018

0.2 Sécurité de l'information en matière de protection des données

Dans cette édition, des informations complémentaires relative au RGPD ont été ajoutées au BSG existant, afin d'intégrer ces deux aspects dans un documents unique.

Comme cela a déjà été expliqué dans l'introduction, une différence est donc faite entre

- sécurité de l'information et
- protection des données personnelles

Pour éviter toute confusion, nous utilisons ci-après "**protection des données**" pour faire référence à la protection et à la gestion des **données à caractère personnel** telles que décrites dans le RGPD, Art.4.1

Si nous utilisons la notion de "sécurité de l'information", il s'agit de mesures plus générales liées à la sécurité des données d'entreprise sous BSG ou telle que reprise dans la norme ISO/IEC 27001.

0.3 Légende

Afin de faire la distinction entre les mesures supplémentaires liées à la protection des données, des codes de couleur sont utilisés pour identifier les contrôles relevant de ce domaine.

0.3.1 BSG

Le contenu qui concerne à la fois la sécurité de l'information et la protection des données est marqué en bleu / noir

BSG et RGPD
Sécurité de l'information et protection des données

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

0.3.2 RGPD

Le contenu qui **ne concerne que** la RGPD est surligné en orange.

Spécifiquement RGPD
Contenu spécifique à la protection des données (RGPD)

0.3.3 Général

Les points d'intérêt généraux, les informations importantes, les avertissements, … sont mis au vert indépendamment de la sécurité de l'information ou la protection des données.

Important - Générale
Point d'attention général ou contenu distinct de BSG ou RGPD

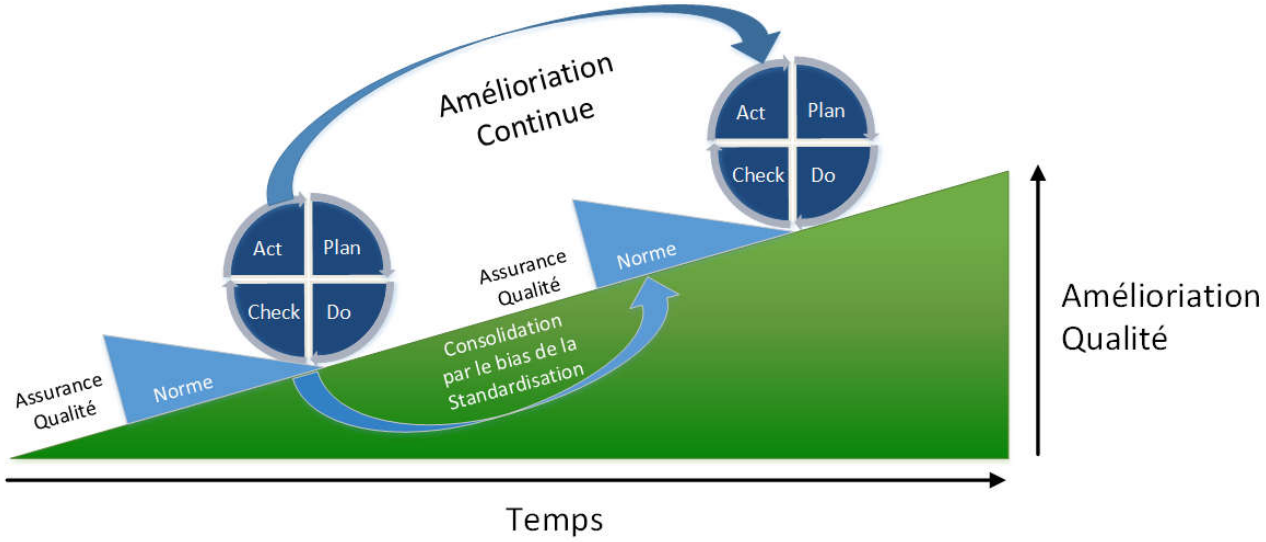
CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

1 Les quatre principes de base d'une gestion de la sécurité de l'information

Il convient de garder à l'esprit **quatre principes** clefs lors de la mise en place d'une bonne gestion de la sécurité de l'information, à savoir:

1. la stratégie et le soutien de la direction
2. l'inventaire des actifs et l'analyse des risques
3. la mise en place des mesures de sécurité
4. L'évaluation des mesures de sécurité

L'évaluation des mesures de sécurité Ces principes de base s'inspirent d'une approche de qualité de la sécurité de l'information qui consiste à continuellement évaluer les actions mises en œuvre afin d'améliorer la qualité (PDCA = Plan, Do, Check, Act).



Important

Après l'implémentation initiale du plan PDCA, l'évaluation continue devient un cycle récurrent dans le but d'améliorer la sécurité.

RGPD

Les 4 principes s'appliquent également directement à la mise en œuvre d'RGPD, telle qu'elle est utilisée par l'autorité Belge de protection des données (APD) dans ses mesures de référence.

Ces principes contiennent **15 points d'attention** qui sont les suivants.

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

1.1 La stratégie et le soutien de la direction

1. **L'implication des dirigeants et des responsables de traitement** est la meilleure façon de soutenir la mise en place de structures opérationnelles, de procédures et de moyens. Cependant, afin que les mesures mis en œuvre soient efficaces, il convient de les communiquer à toutes les parties prenantes de votre organisation.
2. Développer une **stratégie en matière de sécurité et une politique de sécurité** de l'information en adéquation avec la stratégie de l'organisation afin qu'elle supporte les objectifs tout en respectant les dispositions légales et réglementaires.
3. Définir un plan pluriannuel de **formations et de sensibilisation** régulières pour l'ensemble des collaborateurs internes et externes de l'organisation.
4. Intégrer pour tout nouveau **projet une culture de sécurité** et d'analyse de risques dès le début, que ce soit au niveau du développement de nouvelles applications ou de projets de gestion de l'entreprise.
5. Disposer d'un plan de gestion des **incidents de sécurité** majeurs/graves et de crises.
6. Mener une **gestion active et régulière des changements importants** de l'environnement.
7. Disposer d'**un plan de continuité des activités** (PCA).

1.2 L'inventaire des actifs et l'analyse des risques

8. **Identifier les actifs essentiels de l'information** ainsi que leur propriétaire, et ensuite définir les rôles et responsabilités pour toute la chaîne de traitement du risque.
9. **Gérer les risques** pour définir les priorités et mettre en place les mesures appropriées afin de réduire les risques (en les ramenant à un niveau acceptable) et les impacts potentiels liés aux actifs d'information.

1.3 La mise en place des mesures de sécurité

10. Mettre en place **des mesures spécifiques** visant à la sécurisation de l'information de l'organisation qui doivent être validées, communiquées, implémentées et revues.
11. **Gérer les ressources** allouées à la sécurité de l'information et aux infrastructures de façon efficace et efficiente, en ce compris la désignation de responsables de la sécurité de l'information et la désignation du délégué à la protection des données.
12. Mettre en place, avec le soutien de la direction, **une politique de catégorisation des systèmes d'information et des données** sur la base des besoins de confidentialité, d'intégrité et de disponibilité (de l'anglais "*Confidentiality, integrity and availability*" ou *CIA*) et de leurs sensibilités en matière de protection des données et ce, pour toute leur durée de vie. Cette politique devra faire l'objet d'une révision périodique.

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

1.4 Evaluation des mesures de sécurité

13. **Effectuer une évaluation annuelle des mesures de sécurité** afin d'évaluer l'état des lieux sur l'avancement du plan de sécurité, ses améliorations et ajouts éventuels est nécessaire pour toute organisation.
14. **Mesurer**, de façon ponctuelle, **les performances des actions** (points précédents) mises en place mais également l'évolution des menaces et des vulnérabilités afin de s'assurer que les objectifs sont atteints (cycle d'amélioration continue, PDCA)
15. Envisager d'**adapter l'analyse et la gestion des risques** à la lumière des audits et des incidents avérés et des changements importants impactant les activités.

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

2 La stratégie et le soutien de la direction

2.1 L'implication des dirigeants

Le plan de sécurité et de protection des données et ses priorités doivent être présentés, approuvés, validés et soutenus par **la direction de l'organisation** comme responsable final de la sécurité de l'information et de la protection des données.

Pour ce faire, chaque mesure proposée devra comporter une mention de sa priorité et des ressources nécessaires.

Il est important de vérifier que ce plan est en adéquation avec la **stratégie et les objectifs opérationnels de votre organisation**, sans quoi il sera rejeté par la direction.

Dans la présentation à la direction, il faut veiller à mentionner le niveau de sécurité actuel et le niveau désiré après implémentation du plan. La responsabilité de la direction doit être soulignée, et notamment quant à son acceptation du risque.

Ce plan, une fois approuvé par la direction, devra être intégré aux priorités opérationnelles de l'organisation et être communiqué à l'ensemble de l'organisation et à ses parties prenantes afin d'en obtenir la collaboration de toutes les parties.

2.2 La stratégie de la sécurité

La gestion de la sécurité de l'information exige que la direction s'implique, promeuve une culture propice à la sécurité et de protection des données et fasse l'apologie des bonnes pratiques et des mesures de sécurité.

Néanmoins, même s'il est plus facile d'acheter une solution technique que d'essayer de changer la culture de l'organisation, n'importe quelle solution technique ne remplacera pas **l'efficacité et la créativité d'une solution humaine**.

Important
Chacun fera sa part pour améliorer la sécurité si la culture d'entreprise le permet et le stimule. **Le bon exemple de gestion par la direction est donc essentiel à cet égard.**

La gestion de la sécurité de l'information et de protection des données fait partie de toute bonne gestion de l'organisation. Elle fournit aux dirigeants une direction stratégique. Elle s'assure en outre que les objectifs sont atteints, que les risques sont gérés de façon appropriée et que les ressources opérationnelles sont gérées efficacement. Elle mesure aussi la réussite et/ou l'échec du programme de sécurité.

Une identification des rôles et responsabilités de chacun quant à la protection de l'information ainsi que la structure de l'organisation sont des outils indispensables afin de permettre une évaluation des tâches et activités nécessaires à la mise en place de ce plan (définition d'une matrice RACI p.ex.).

Afin d'obtenir une gestion de l'information efficace, il importe que la direction en fixe le cadre afin de guider son développement ainsi que la réalisation du plan de sécurité de l'information.

Ceci permettra à l'organisation de gérer ses actifs essentiels (infrastructure, données, …) tout en les protégeant de risques importants.

Afin d'améliorer l'alignement de cette stratégie sur les objectifs de l'organisation, la stratégie opérationnelle devra fournir les éléments clés pour l'analyse de risques comme, par exemple, les procédures opérationnelles et les ressources critiques pour la stratégie de sécurité de l'information.

Les mesures de sécurité sont la résultante de l'analyse de risques et définissent les grandes lignes du programme de sécurité de l'organisation: les ressources nécessaires, les contraintes, …

Le développement du programme de sécurité de l'information devra également prévoir des outils d'évaluation des mesures mises en place, de leur révision et d'adaptation si nécessaire.

Un **rapport complet et régulier de l'état d'avancement** aux dirigeants permettra de décider d'adaptations et de mesures correctives afin d'atteindre l'état de sécurité souhaité par la stratégie de l'organisation.

L'information aux dirigeants leur permettra d'évaluer les ressources nécessaires pour la sécurité de l'information et donc d'accepter les mesures minimales à prendre pour s'assurer de la sécurité de l'information.

Ces mesures minimales sont adaptées au niveau d'importance des actifs à protéger et à leur degré de sensibilité. Ces mesures de base sont définies en termes de ressources, de procédures et de moyens techniques; elles sont souvent inspirées de standards ainsi que du respect des lois et règlements nationaux et sectoriels.

3 Inventorier vos actifs essentiels & l'analyse de risques

3.1 Définition des actifs

Pour la sécurité de l'information, les actifs essentiels sont généralement considérés comme "toutes les ressources qui ont une valeur pour l'organisation et qui doivent être sécurisées". À cette fin, un aperçu clair de la valeur et de l'importance des données traitées est nécessaire (voir informations de catégorisation).

Les actifs ne se limitent pas uniquement à l'infrastructure IT ou à des moyens tangibles, mais ils s'appliquent aussi aux données, à des personnes et des moyens intangibles comme des processus, des procédures, la connaissance et l'expertise.

L'application de la **protection des données** (RGPD) diffère en ceci, car **la définition des actifs essentiels** est définie dans la RGPD elle-même.

Plus spécifiquement, l'article 4.1 détermine le contenu des "**données personnelles**". De plus, l'article 9.1 de la RGPD contient également la définition de **catégories particulières** de données personnelles.

3.2 L'inventaire des actifs

La première étape **consiste à dresser un inventaire des actifs essentiels** au fonctionnement de votre organisation.

Il est recommandé de commencer par exemple par les "actifs essentiels" connus et identifiés par la direction.

Les différentes itérations de votre plan vous permettront d'enrichir progressivement cet inventaire, de le compléter, de l'étoffer.

Le RGPD impose par ailleurs de disposer d'un inventaire des traitements de données à caractère personnel « registre des activités de traitement ». Les informations minimales nécessaires sont décrites à l'article 30 du RGPD. Dans la majorité des cas, un traitement de données correspondra à un système d'information et les actifs identifiés correspondront aux éléments (IT, personnel, infrastructure,…) nécessaire pour réaliser ce traitement.

3.2.1 Les étapes

Afin de dresser l'inventaire:

- définissez/identifiez, en collaboration avec la direction et les départements, les différents "actifs essentiels";
- au besoin, rencontrez les personnes responsables de ces différents actifs afin de mieux les cerner/définir;
- dressez-en la liste;
- soumettez cette liste, de façon formelle, à la direction pour approbation. Cela permettra de l'impliquer dans votre démarche (par exemple via un PV d'approbation ou un document signé par la direction).

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

3.2.2 Le résultat

Il existe différents types d'actifs essentiels au sein de toute organisation. En voici une liste non exhaustive à titre d'exemple:

- Les **actifs primaires**, à savoir:
  - L'information, les données, les services, les processus clés, les personnes clé,
  - Données personnelles absolument nécessaires pour assurer le service de base de l'organisation
- Les **actifs secondaires** supportant les actifs primaires comme
  - Les systèmes IT, réseau, télécommunications
  - Données personnelles requises pour les processus de support tels que les newsletters, le marketing, etc.

N'essayez pas d'avoir une liste exhaustive, concentrez-vous sur l'essentiel.

Il est préférable de démarrer le processus avec uniquement un nombre limité d'actifs que d'essayer de les lister tous. Vous risquez en effet grandement que la liste soit obsolète lorsque vous aurez terminé l'exercice.

Important
Ce qui est important, c'est de démarrer le processus, de l'améliorer continuellement au fur et à mesure.

La Méthode Optimisée d'analyse des risques Cases (Monarc)[2] propose une approche d'identification des actifs. L'on retrouve aussi une approche encore plus détaillée dans la norme ISO/IEC 27005.

[2] http://monarc.lu/

3.3 L'analyse de risques en 6 points

Pour chaque actif essentiel, il est important d'effectuer une analyse de risques.

Il est à noter que la section 3 du RGPD de l'Union européenne explicite la nécessité de réaliser une analyse de risques pour tout traitement de données à caractère personnel à risque.

Alors que dans le cadre d'une approche usuelle de gestion des risques on considère les risques pour l'organisation. Dans le cadre du RGPD, on doit considérer les risques pour les individus dont les informations sont traitées. Le traitement de ces deux aspects est complémentaire. Ils seront abordés conjointement et pourront le plus souvent conduire à des traitements du risque commun.

3.3.1 Établissez le contexte de votre organisation

- Profil de risque (facteurs interne & externe)
  - Quel est le contexte spécifique de votre organisation/secteur spécifique ?
  - Propriétés de l'organisation ?
  - Les components internes ou externes lesquels influencent le risque?
  - Quels sont les types de données traitées (données personnelles et autres)
  - Pour chaque type de donnée, quels sont les risques pour l'organisation et pour les personnes concernées
- Appétit de risque (choix de l'organisation)
  - Quel est le niveau de risque acceptable pour votre organisation?
  - Quel est le niveau de risque acceptable pour les personnes concernées?

3.3.2 Modélisation du contexte

- Identification des actifs essentiels
  - Rassembler les informations comme par exemple le flux du processus, les infrastructures, les bases de données, les brevets, les personnes clés, les transferts de données vers des tiers, …
  - Rassembler les contrats/protocoles avec les parties tierces (fournisseurs, sous-traitants, IT provider, cloud, etc., toute partie externe qui gère pour votre organisation des infrastructures, applications ou bases de données).
- Identification des risques, vulnérabilités, menaces, …
  - Identifier les risques possibles au niveau de la confidentialité, l'intégrité, la disponibilité, la traçabilité, la non-répudiation et l'authenticité des données ainsi que les risques de compliance RGPD (légalité, proportionnalité, opportunité, transparence, exacte, mise à jour,…).
  - On décrit généralement la notion de "risque" comme
    - la possibilité ("probabilité")
    - qu'une menace déterminée/donnée (profitant d'une vulnérabilité) se présente et profite d'une faiblesse,
    - avec pour conséquence un impact déterminé ("gravité").

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

  - Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa vraisemblance.
- Processus de comparaison des résultats de l'analyse des risques avec les critères de risque afin de déterminer si le risque et/ou son importance sont acceptables ou non.

3.3.3 Évaluation et traitements des risques

- Identifier les mesures de sécurité organisationnelles, opérationnelles et techniques déjà en place pour sécuriser l'actif en question ou minimiser l'impact sur la personne concernée dans la cadre de la protection des données.
- Identifier les mesures de sécurité organisationnelles, opérationnelles et techniques supplémentaires pour renforcer la sécurité et la protection des données.
- Évaluer le niveau de risque résiduel. Est-il à un niveau acceptable pour votre organisation ?

En matière de gestion des risques, on peut opérer une distinction entre le risque "inhérent" et le risque "résiduel".

- **Le risque "inhérent**" renvoie à la probabilité qu'un impact négatif se produise lorsqu'aucune mesure de protection n'est prise.
- **Le risque "résiduel"** renvoie, au contraire, à la probabilité qu'un impact négatif se produise, malgré les mesures qui sont prises pour influencer (limiter) le risque (inhérent).

L'analyse du risque résiduel souhaité vous sera utile pour sélectionner et développer des actions/mesures à prendre, ce qui vous permettra d'obtenir un risque résiduel acceptable comme défini par les propriétaires fonctionnels et/ou les responsables de traitement .

3.3.4 Implémentation des mesures

L'implémentation des mesures peut inclure (selon le principe de "PPT"):

1. les **P**ersonnes ("People")
2. les **P**rocessus et procédures ("Processes")
3. la **T**echnologie ou l'infrastructure technique ("Technology or Systems")

3.3.5 Monitoring: évaluer l'implémentation des mesures & leurs effets sur la diminution des risques

Il n'est pas suffisant d'implémenter des mesures; il est nécessaire de les évaluer régulièrement.

3.3.6 Enrichir l'analyse de risques avec des nouveaux actifs (itérer le point 1)

Votre analyse de risques est un élément dynamique qu'il faudra continuellement mettre à jour au vu des incidents, des modifications du traitement, de la maintenance de l'outil, de la modification des actifs essentiels, de l'adaptation règlementaire ou légale, ou de la disponibilité des ressources, des personnes, du temps ou du budget.

3.4 Quelle méthode utiliser?

La Méthode Optimisée d'analyse des risques Cases ("Monarc") propose une approche d'analyse de risques. L'on retrouve aussi une approche plus générique dans la norme ISO 27005.

Votre analyse de risques peut être très simple, comme elle peut être très détaillée…

Tout dépend de la taille de votre organisation, de la complexité des projets et de la sensibilité des données que vous traitez.

Ne sous-estimez pas le travail car, même si un projet paraît simple, les risques y afférents peuvent être importants. Il n'y a donc pas de proportionnalité entre la taille du projet et les risques liés à ce projet. Afin de vérifier l'exactitude et l'exhaustivité de votre analyse de risques, demandez à différentes personnes de votre organisation de la relire.

En règle générale, toute organisation est libre de choisir la méthodologie qu'elle souhaite utiliser.

Toutefois, l'utilisation d'une méthodologie comparable par d'autres organisations offre d'importants avantages.

Le résultat de votre analyse de risques sera à la base de votre plan de sécurité. Pour ce faire, vous devrez fixer en priorité les mesures de sécurité à mettre en place afin d'obtenir un plan d'implémentation à faire valider par la direction.

Cette démarche s'applique également à la protection des données. Cependant, comme indiqué précédemment, il est important de savoir que l'analyse des risques dans le cadre du RGPD fait l'objet d'une attention particulière sous la forme d'une analyse d'impact sur la protection des données (AIPD).

Pour la mise en œuvre de l'AIPD, il est souvent fait référence à la norme ISO29134 (Évaluation de l'impact sur la vie privée). La bonne nouvelle est que cela s'intègre parfaitement dans l'histoire plus large de la gestion des risques informatiques (ISO27005) et que Monarc est parfaitement équipé pour le mettre en pratique. La récente publication de la norme ISO/IEC 2770:2019 (Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices) permet d'intégrer les objectifs de sécurité de l'information avec la protection des données.

Dans leur recommandation sur le DPIA, la APD se réfère également à cette norme, bien qu'ils insistent sur le fait que chaque contrôleur reste libre dans son choix.

Plus d'informations à ce sujet:

https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2018_0.pdf (numéro 54 et note de bas de page 91 associée).

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

3.5 L'analyse de risques dans l'approche gestion de projets

La sécurité doit être pensée à chaque étape de tout processus de développement de votre projet (sécurité par défaut et par design) Veillez à adapter votre politique de gestion de projets au niveau de la gestion de projets pour y inclure l'analyse de risques et les mesures sécurité et de protection des données à implémenter.

N'oubliez pas également que l'analyse de risques des systèmes TIC doit être effectuée dès le début du projet de développement d'une nouvelle solution ("security & privacy by design"). Elle revêt donc un caractère évolutif ! Ceci signifie qu'elle est sujette à des modifications en cours d'élaboration du projet.

Dans le cadre du RGPD, ce souci de gérer les risques est matérialisé par l'exigence de protections des données personnelles dès la conception et par défaut (art. 25 RGPD)

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

4 Mise en place des mesures de sécurité

Les mesures minimales de sécurité sont recommandées pour toute organisation, quelle que soit sa taille. Certaines ne seront pas applicables au vu du contexte de l'organisation. Cependant, ces normes étant créées pour l'ensemble du service public, elles sont adaptables à la taille et au contexte de votre organisation.

Afin de garder un lien avec les mesures décrites ci-après, l'ordre du standard ISO 27001 a été utilisé.

4.1 Politique de sécurité

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation doit disposer d'une politique de sécurité approuvée et soutenue par la direction.	Chaque organisation mettra en place une (des) politique(s) de sécurité de l'information, actualisée(s) et approuvée(s) par la direction.
	La direction devra être tenue au courant régulièrement de l'état des mesures mises en œuvre.
	La politique de sécurité de l'information doit être disponible et consultable par les parties concernées.
	La direction doit être régulièrement informée de l'état des lieux des mesures mises en œuvre.
	La politique de sécurité de l'information doit être réévaluée par la direction au moins une fois par an pour rester pertinente et conforme à la réalité.

4.2 Organisation de la sécurité

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation mettra en place un système de gestion des risques.	Un processus de gestion des risques sera documenté, approuvé et revu périodiquement.
	Un registre des actifs et des risques y afférents ainsi que des mesures prises (réduction, acceptation, transfert) sera tenu à jour.

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
La sécurité de l'information sera intégrée dans la gestion des projets (Sécurité dès la conception - "security by design") afin d'intégrer le plus tôt possible les aspects de sécurité.	Un processus documenté de gestion des risques de sécurité de l'information sera mis à jour et l'on veillera à sa mise en application.
Afin de mettre à jour les connaissances et de favoriser les échanges sur les dernières tendances en matière de sécurité de l'information, il sera nécessaire de participer aux forums spécialisés abordant les questions de sécurité de l'information.	Une veille technique des forums spécialisés en sécurité de l'information sera implémentée.
Afin que ces mesures organisationnelles soient appliquées, chaque organisation (in)formera son personnel et les tiers opérant sous sa responsabilité.	Un plan de formation au risque de sécurité sera développé, maintenu à jour et suivi.
	Le plan de sécurité de l'information est disponible et peut être consulté par les personnes concernées.
	Une formation permanente du personnel et des tiers sur sa politique de sécurité et de protection des données, ainsi qu'une procédure de sanctions pour non-respect seront implémentées.
Chaque organisation veillera à désigner et mandater un responsable de la sécurité.	Un responsable en sécurité de l'information avec un mandat clair sera désigné.
Chaque organisation disposera d'un tableau de bord permettant de mesurer son niveau de sécurité par rapport aux objectifs fixés par la stratégie de l'organisation.	Un tableau de bord revu, présenté à la direction et permettant d'évaluer l'état de la sécurité de l'organisation sera mis en œuvre.
Un code de conduite et de bonnes pratiques en matière d'utilisation des systèmes d'information sera élaboré, approuvé et communiqué.	Mettre en place un code de conduite pour tout utilisateur lors de la sélection, la gestion et le désengagement de vos employés, et assurément pour ceux qui ont accès à des données sensibles ou à des systèmes critiques.

Mesure de sécurité	Mesures minimales à mettre en place
	Ce code de conduite devra comporter les éléments suivants: ▪ Gestion des accès/autorisations ▪ Révocation des droits ▪ Confidentialité des données ▪ Systèmes d'accès physique aux bâtiments & infrastructures ▪ Systèmes d'accès & confidentialité des données d'accès ▪ Procédures pour définir l'utilisation correcte des outils de travail mis à disposition (appareils mobiles, télétravail, catégorisation des données,…) ▪ Les mesures mises en œuvre pour le contrôle des opérations (Accès, stockage destruction, accès à distance, journalisation, …)
	Publier, communiquer le code de conduite et de le rappeler régulièrement (campagnes de sensibilisation).
Un plan d'information & de formation sera adopté.	Le plan devra inclure les relations avec des tiers et les autorités.
	Une culture de sécurité intégrant la sécurité dans les processus de développement sera définie et promue.
Chaque organisation définira les règles et mesures de sécurité d'usage des supports média amovibles.	Une procédure d'utilisation des outils mobiles sera adoptée.
Une politique d'accès, de gestion des informations à distance (télétravail) sera adoptée.	Une procédure d'accès, de gestion des informations à distance (télétravail) sera adoptée.

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation doit identifier les rôles et responsabilités des différents acteurs dans la sécurité de l'information.	Une identification des rôles et responsabilités de chacun quant à la protection de l'information ainsi que la structure de l'organisation sont des outils indispensables afin de permettre une évaluation des tâches et activités nécessaires à la mise en place de ce plan (définition d'une matrice RACI p.ex.).

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation mettra en place un système de gestion des risques pour la gestion des données personnelles.	Un processus de gestion des risques pour la gestion des données personnelles est documenté, approuvé et évalué périodiquement. Ce processus s'intègre autant que possible avec le processus général de gestion des risques. Si nécessaire, cela peut être combiné avec le système de gestion des risques pour la sécurité de l'information.
	Une classification est établie qui réparti les données personnelles en différentes catégories, chacune devant être protégée de manière appropriée. ▪ Données personnelles sensibles ▪ Données personnelles normales ▪ Pas de données personnelles
Configurer et gérer le registre de traitement RGPD	(Réf. RGPD Art. 30.) Un registre des différents activités de traitement des données à caractère personnel sera tenu, y compris: ▪ Les coordonnées du responsable de traitement et de la coresponsable ▪ Coordonnées du DPO ▪ fins de traitement ▪ Catégorie de données traitées ▪ Catégorie de personnes impliquées ▪ Mesures de protection applicables …

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
	Un cycle de vie des données personnelles est défini, y compris (Ref. RGPD Art 4.2°) ▪ Création ▪ La collecte ▪ Approvisionnement ▪ Traitement ▪ Transport et distribution ▪ Stockage ▪ Archivage ▪ Destruction ▪ …
	Le registre de traitement RGPD contient également ▪ Source de données ▪ Méthodes de récolte des données ▪ Raison de traitement ▪ Type de traitement ▪ (Catégorie de) destinataires de données ▪ ▪…
Chaque organisation veille à ce qu'un délégué à la protection des données (ci-après désigné DPO) doté d'un mandat clair soit désigné et mandaté.	RGPD Art. 37 1) *"Le responsable du traitement et le sous-traitant désignent un délégué à la protection des données lorsque:* *a) le traitement est effectué par une autorité publique"*
	Un responsable de la protection des données doté d'un mandat clair sera nommé.
La protection des données sera intégrée à la gestion du projet (protection des données par conception) afin d'intégrer les aspects de sécurité le plus rapidement possible.	RGPD Art. 25 requiert le principe de *"Protection des données dès la conception et protection des données par défaut"* C'est pourquoi il est important d'inclure la protection des données lors du démarrage de nouveaux projets ou de l'adaptation d'opérations existantes.

Mesure de sécurité	Mesures minimales à mettre en place
Pour mettre à jour les connaissances et promouvoir l'échange des tendances en matière de protection des données, il sera nécessaire de participer à des forums spécialisés et à des canaux d'information traitant de la protection des données.	Les tâches et les ordres du jour nécessaires sont attribués, planifiés et exécutés afin de consulter des informations sur les newsletters, blogs, forums en ligne, etc., qui fournissent des informations actualisées sur la protection des données.
	Les tâches et les ordres du jour nécessaires sont attribués, planifiés et exécutés afin de consulter des informations sur les newsletters, blogs, forums en ligne, etc., qui fournissent des informations actualisées sur la protection des données.
Pour s'assurer que les mesures organisationnelles nécessaires sont mises en œuvre, chaque organisation informe son personnel et les tiers travaillant sous sa responsabilité.	Un plan de formation à la protection des données est développé, mis à jour et suivi.
	Une formation continue du personnel et des tiers en ce qui concerne les politiques de sécurité et de protection des données, ainsi qu'une procédure de sanction pour non-conformité seront mises en œuvre.
Chaque organisation dispose d'un tableau de bord pour mesurer et contrôler l'état et maturité de protection des données par rapport aux objectifs de sa stratégie.	Un tableau de bord est évalué, présenté à la direction et utilisé pour évaluer l'état de la protection des données dans l'organisation. (Incl. nombre de modifications, incidents internes et externes, fuites de données, nombre de demandes de consultations irrégulières,...)
Un code de conduite et de bonnes pratiques pour l'utilisation de données à caractère personnel seront développés, approuvés et communiqués.	Établissez un code de conduite pour chaque utilisateur lors de la sélection, de la gestion et de l'accès de vos employés, et certainement pour ceux qui ont accès à des données sensibles ou à des systèmes critiques.

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
	Ce code de conduite doit contenir les éléments suivants: ▪ Contrôle d'accès / gestion des autorisations ▪ Retrait des droits ▪ Confidentialité des données. ▪ Accès physique aux bâtiments et aux infrastructures ? ▪ Systèmes d'accès et confidentialité des données d'accès ▪ Procédures permettant de déterminer l'utilisation correcte des outils de travail mis à disposition (tels que les appareils mobiles, le télétravail, la classification des données, etc.) ▪ Quelles mesures ont été prises pour contrôler les activités (accès, destruction de stockage, accès à distance, journalisation) ?
	Communiquez le code de conduite et de le répéter régulièrement (par le biais de campagnes de sensibilisation).
Un plan d'information et de formation sera approuvé.	Le plan doit inclure les relations avec les tiers et les autorités.
	Une culture de la sécurité sera définie et promue, avec l'intégration de la sécurité dans les processus de développement.
Les règles d'accès aux données sont déterminées.	Une procédure d'accès aux données personnelles et aux données personnelles sensibles est élaborée et contrôlée.
Chaque organisation doit identifier les tâches et les responsabilités des différents acteurs de la protection des données.	L'identification des rôles et des responsabilités en matière de protection des données, ainsi que la structure de l'organisation, sont des outils essentiels pour évaluer les tâches et activités requises pour mettre en œuvre ce plan (définition d'une matrice RACI, par exemple).

4.2.1 Registre des activités de traitements

Voir la recommandation APD (à partir du note 38):

https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_06_2017_0.pdf

Il est important de faire la distinction entre les données d'informations devant figurer dans le registre sous RGPD lui-même (énumérées à l'article 30.1 du RGPD) et les informations utiles et souhaitables, mais non obligatoires.

Voir également page 15 de la brochure APD SME:

https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/PME_FR_0.pdf

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

4.3 La sécurité des ressources humaines

Mesure de sécurité	Mesures minimales à mettre en place
Une politique relative à la gestion des collaborateurs (internes et/ou externes) sera adoptée.	Des procédures couvrant les aspects suivants seront développées: Avant l'emploi: ▪ Procédures d'engagement et mesures y afférents Pendant l'emploi: ▪ Tous les collaborateurs internes et externes doivent adhérer au code de conduite de l'organisation. La résiliation ou la modification de l'emploi: ▪ Les responsabilités et les obligations relatives à la sécurité de l'information demeurent après la résiliation ou le changement d'emploi et ces termes doivent être clairement communiqués et intégrés dans le processus de gestion des collaborateurs (internes ou externes).
Réglementation de l'emploi	Une politique doit être définie, qui définit clairement les responsabilités de l'organisation, des employés internes et externes en matière de sécurité de l'information et de protection des données.

Mesure de sécurité	Mesures minimales à mettre en place
La politique pour les employés (internes et externes) contient une bonne protection juridique et / ou contractuelle des données personnelles.	Conformément à l'article 88 ("Traitement de données dans le cadre des relations de travail "), des règles et des accords ont été établis pour protéger les droits et les libertés des employés / fonctionnaires dans le cadre des relations de travail.

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
Procédure de recrutement	Tout au long de la carrière des membres du personnel, du recrutement au licenciement, une attention suffisante doit être accordée à la protection des données personnelles
Réglementation de l'emploi	Voir ISO27701 (traduit) **"6.10.2.4 Accords de confidentialité ou de non-divulgation** *Les audits, les instructions de mise en œuvre et les autres informations spécifiées dans les normes ISO / IEC 27002: 2013, 13.2.4 et les directives supplémentaires suivantes s'appliquent:* **Les directives supplémentaires de mise en œuvre pour 13.2.4, accords de confidentialité ou accords de confidentialité de l'ISO/CEI 27002: 2013 sont les suivantes:** *L'organisation doit s'assurer que les personnes opérant sous son contrôle et ayant accès aux informations personnelles ont une obligation de confidentialité. L'accord de confidentialité, qu'il fasse partie d'un contrat ou séparément, doit spécifier la durée pendant laquelle les obligations doivent être remplies.* *Lorsque l'organisation est un processeur PII, un accord de confidentialité, sous quelque forme que ce soit, entre l'organisation, ses employés et ses agents doit garantir que les employés et les agents adhèrent aux politiques et procédures de traitement et de protection des données. "*

4.4 Sensibilisation, formation, développement & Communication

Mesure de sécurité	Mesures minimales à mettre en place
Un plan de formation, de développement et de communication sera défini afin que tous les collaborateurs de l'organisation, internes et externes, suivent, dans la mesure du possible, la formation en matière de sécurité de l'information et soient régulièrement informés sur les adaptations apportées aux directives et procédures.	Des procédures seront élaborées pour les aspects suivants: ▪ Un programme visant à sensibiliser les employés à la sécurité de l'information, tant en interne qu'en externe; ▪ Le programme doit être organisé à intervalles réguliers (de préférence 1 ou 2 fois par an ou plus) de sorte que les nouveaux employés soient également intégrés au programme à temps; ▪ Cette information doit toujours être accessible aux employés de façon simple et harmonieuse;
Un plan de communication sera défini pour que toutes les parties intéressées de l'organisation, en interne et en externe, reçoivent les informations nécessaires sur la sécurité de l'information, le cas échéant, et soient régulièrement informées des adaptations apportées aux lignes directrices et aux procédures.	Des procédures seront développées pour les aspects suivants: ▪ Identification des parties impliquées et mode de communication adéquat ▪ Prévoir de régulièrement tenir au courant les parties des adaptations apportées aux directives et procédures

Mesure de sécurité	Mesures minimales à mettre en place
Vadémécum avec la terminologie RGPD	Dans le cadre de la politique de sécurité, un vadémécum est disponible pour les parties impliquées. Il explique et consolide la terminologie utilisée pour la mise en œuvre de la RGPD, afin que tout le monde utilise le même vocabulaire.

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
Un plan de formation et d'éducation sera défini de manière à ce que tous les employés de l'ensemble de l'organisation, qu'ils soient internes ou externes, reçoivent l'instruction et la formation nécessaires à intervalles réguliers ▪ **sur la RGPD et la protection des données,** ▪ **dans les mesures applicables à leurs fonctions/ poste leur rôle et leur responsabilité à cet égard,** **et être tenu informé des modifications apportées aux directives et procédures.**	Des procédures seront développées pour les aspects suivants: ▪ Un programme de sensibilisation au RGPD et à la protection des données (en mettant l'accent sur les données personnelles) parmi les employés, à la fois en interne et en externe. ▪ Le programme doit être répété à intervalles réguliers (de préférence 1 ou 2 par an ou plus), afin que les nouveaux employés soient inclus dans le programme à temps. ▪ Cette information doit être disponible pour chacun des employés o être clairement comprise o être adaptée au niveau de l'employé o toujours accessible de manière simple et fluide. ▪ Le signalement d'éventuels incidents de sécurité doit être rendu possible sans que les employés fassent obligatoirement l'objet de sanction ou des représailles
Un plan de communication sera défini de manière à ce que toutes les parties intéressées de l'organisation, tant internes qu'externes, reçoivent les informations de protection des données nécessaires, le cas échéant, et soient régulièrement informées des modifications apportées aux directives et aux procédures.	Des procédures seront développées pour les aspects suivants: ▪ Identification des parties impliquées et des moyens de communication appropriés. ▪ Prévoyez de tenir les parties informées à intervalles réguliers des ajustements apportés aux directives et aux procédures. ▪ Prévoyez de tenir les parties régulièrement informées de l'état de l'environnement de protection des données, y compris d'un bref aperçu des incidents et de leurs tendances. ▪ Il est également essentiel d'intégrer une incitation à l'amélioration continue
Préparez une déclaration de protection des données expliquant quelles données sont traitées, comment et les mesures de protections mises en œuvre.	Avant et au plus tard au moment de la collecte des données, des informations claires doivent être fournies à la personne concernée,

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
	La déclaration de protection des données doit pouvoir être consultée ou demandée à tout moment par la personne concernée à une date ultérieure.
Procédure de communication pour l'exercice des droits de la personne concernée	La personne concernée doit recevoir une explication claire de la manière dont elle peut exercer ses droits en vertu de la RGPD, tels que le droit à l'information, la rectification, l'effacement des données, la limitation du traitement, la transférabilité, l'objection au traitement et au profilage, etc.

4.5 La gestion des actifs

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation établira un inventaire de ses actifs essentiels, quelle que soit sa catégorie (information, données, transmission, application, réseaux, processus, systèmes, …).	Chaque asset/actif sera détaillé dès la conception ("by design") et tous les éléments seront repris afin de bénéficier d'une cartographie de l'architecture de l'information de l'organisation ("by default").
	Chaque élément de cet inventaire sera assigné à un responsable (avec son backup) dont les données de contact seront tenues à jour.
	Pour chaque élément d'actif, les accès et autorisations accordés seront fixés. Les accès et autorisations seront octroyés en tenant compte du principe "need-to-know/need-to-use".
	Lorsque le responsable est une personne extérieure à la société (fournisseur de logiciel, sous-traitant), les références du contrat seront reprises dans l'inventaire ainsi que les données de contact en cas d'urgence.
	Cet inventaire sera sécurisé mais connu des personnes clés de l'organisation et de celles devant gérer un incident.

Mesure de sécurité	Mesures minimales à mettre en place
Un inventaire des systèmes d'information sera tenu à jour.	Un inventaire des systèmes d'information et des services clients (par exemple: liste des applications et utilisateurs des applications/données sur le serveur)
	L'inventaire de l'interdépendance entre les systèmes au niveau technique et fonctionnel sera tenu à jour.
	La désignation du (des) responsable(s) du système ainsi que les données de contact (personnel interne, fournisseur ou sous-traitant) sera tenu à jour.
	La configuration des systèmes est documentée
	Les procédures de backup, de restauration et d'archivage des systèmes seront tenues à jour.
	L'inventaire de la connectivité et la redondance
	Les procédures de mise en production, changements, mises à jour et maintenance des systèmes: versioning, change & processus maintenance & mesures de sécurité.
	Les procédures de login & monitoring des systèmes
	Procédures pour destruction et/ou décommissionnement d'un actif essentiel
	Pour chaque élément de l'infrastructure, les moyens de protection seront détaillés et assignés à un responsable déterminé. Attention de bien distinguer les personnes ayant une responsabilité opérationnelle de celles qui sont responsables au niveau du développement et du test.

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation veillera à mettre en place une procédure de gestion des actifs de l'information en tenant compte de l'importance des données de l'organisation:	Une catégorisation des informations qui tient au minimum compte de la confidentialité, de l'intégrité, de la disponibilité et de l'authenticité requises pour cette information sera adoptée.
	Une procédure de marquage de cette information sera adoptée.
	Une procédure de manipulation de supports amovibles sera adoptée.
	Une procédure de diffusion, de stockage, d'archivage et de destruction (data life cycle management) sera adoptée.
Chaque organisation mettra en place les mesures de sécurité des données sensibles et des systèmes d'information.	Des mesures de sécurité seront adoptées pour les systèmes en fonction de la catégorisation des données.
	Définition des règles/moyens de confidentialité, intégrité et disponibilité des données et des systèmes d'information
Chaque organisation mettra en place les mesures de sécurité régissant les moyens de communication électronique.	Des mesures de sécurité concernant l'utilisation des moyens de communication électroniques seront adoptées.

Mesure de sécurité	Mesures minimales à mettre en place
Les données personnelles sont suffisamment protégées sur la base de l'évaluation des risques	Comme indiqué à l'article 32 d'RGPD, l'organisation doit prendre les mesures techniques et organisationnelles appropriées pour que le traitement se déroule selon les règles
	Différentes catégories de données à caractère personnel ont été définies, sur la base desquelles des mesures de protection sont mises en œuvre.

4.6 Le contrôle d'accès

Mesure de sécurité	Mesures minimales à mettre en place
L'organisation définira par actif (au sens large du terme) les règles claires d'accès.	De manière générale pour l'accès aux actifs essentiels, un identifiant partagé ne sera pas autorisé.
	Les niveaux d'authentification utilisés par l'organisation seront établis en adéquation avec la catégorisation de l'information déterminée dans l'analyse de risques.
Un registre des autorisations d'accès sera tenu et mis à jour par l'organisation.	Ce registre sera régulièrement revu et mis à jour.
	Ce registre permettra une administration correcte des droits d'accès, leur suivi et leur mise à jour.
	Il sera nécessaire qu'un responsable délivre une autorisation sur la base de ces différents critères (à définir par l'organisation: accréditation service, contrat)
Les utilisateurs seront clairement formés et informés de leurs devoirs & responsabilités.	Une attention particulière sera accordée à la formation et l'information sur les moyens d'accès, et notamment les mots de passe. (Reprendre les éléments pour un mot de passe fort, non partagé, ne pas écrire le mot de passe,

Mesure de sécurité	Mesures minimales à mettre en place
	ne pas utiliser un même mot de passe pour des usages pro & privés, …)
Pour chaque élément de l'inventaire (renforcement des mesures de sécurité, rapport à une autorité)	Les actions seront monitorées au moyen de log, dont l'accès sera sécurisé et uniquement accessible aux personnes identifiées par la direction.
	Tout acte suspect ou tout incident sera rapporté et investigué, et un journal de bord des investigations sera tenu afin de déterminer si des actions subséquentes sont nécessaires.
	Un système de détection des accès non autorisés sera tenu.
Quelques cas particuliers:	Les éléments de communication du réseau seront parties prenantes de cet inventaire et considérés comme des éléments critiques de l'architecture de l'information.
	Un élément supplémentaire sera apporté à la connectivité: afin d'assurer la continuité des opérations de l'organisation, la connectivité sera doublée.
Contrôle d'accès aux données personnelles	Sur la base de la classification / catégorisation des données personnelles, des processus et des procédures doivent être mis en place pour garantir que ▪ Il y a un contrôle d'accès sur les données avec les journaux ▪ Des méthodes d'authentification suffisamment fortes sont utilisées Les employés qui quittent l'entreprise peuvent ne plus avoir accès aux données personnelles dans l'entreprise

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
Vérification de l'identité de la personne voulant exercer ses droits	Un processus qui garantit l'identification de la personne concernée lorsque celle-ci souhaite exercer ses droits, comme le prévoit la RGPD. Note importante : Une implémentation défectueuse ou incorrecte peut entraîner des fuites de données, il est donc très important de traiter cette question avec beaucoup de soin.

4.7 La cryptographie

Mesure de sécurité	Mesures minimales à mettre en place
Si des mesures cryptographiques sont mises en œuvre, l'organisation détaillera:	Documentation de ▪ Catégorisation des actifs ▪ Type de mesure (données en cours de transport, données au repos, données en cours d'exécution, etc.) ▪ Niveau de risque ▪ Catégorie de mesure cryptographique utilisée ▪ Type de crypto algorithmes ▪ Validité des clés et des certificats ▪ …
En règle générale, l'accès aux actifs essentiels doit être basé sur des accès individuels. Le partage de codes d'accès n'est pas permis.	Une mesure de sécurité concernant l'utilisation de la cryptographie doit être mise en place, validée, communiquée et maintenue.
Key management	Une procédure documentée concernant la gestion, l'utilisation, la protection et la durée de vie des clés cryptographiques doit être mise en place.

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

	Mesures minimales à mettre en place
Les données personnelles sont suffisamment protégées lors du stockage, du transport et de l'utilisation des données personnelles	Comme décrit dans l'article 32 du RGPD, les données personnelles doivent être protégées de manière appropriée pendant le stockage, le transport et l'utilisation, par le biais d'un cryptage et d'un pseudonymisation ou par toute autre mesure permettant de garantir le niveau de protection approprié.

4.8 La sécurité physique et environnementale

Mesure de sécurité	Mesures minimales à mettre en place
Espaces sécurisés	Toute organisation doit exclusivement limiter l'accès aux bâtiments et locaux aux personnes autorisées et effectuer un contrôle à ce sujet tant pendant qu'en dehors des heures de travail.
Protection des appareils	Toute organisation doit prendre des mesures de prévention contre la perte, l'endommagement, le vol ou la compromission des actifs de l'organisation et contre l'interruption des activités de l'organisation.
Politique "Clear screen"	Utilisez l'économiseur d'écran et les délais d'attente sur les écrans pour empêcher la lecture d'informations en l'absence
Politique "Clear desk "	S'assurer qu'aucune information, papiers et documents ne sont laissés sans surveillance sur les lieux de travail des employés

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

4.9 La sécurité liée aux opérations

Mesure de sécurité	Mesures minimales à mettre en place
Pour chaque élément d'actif	Login & monitoring avec rapportage des incidents et des mesures de sécurité prises
Un inventaire de l'environnement de test sera dressé.	L'environnement de test sera clairement dissocié de l'environnement de production. Il détaillera: ▪ Les autorisations ▪ Les logs ▪ Le scénario "fall back" pour updates et change ▪ Les tests & updates effectués avec timing & log
Les mesures techniques mises en place pour l'architecture seront au minimum:	▪ Antimalware/antivirus mis à jour ▪ Système de détection des intrusions ou des accès non autorisés/software non autorisés ▪ Procédures de blocage/isolement pour anomalies/accès non autorisé, … ▪ Up to date hardware & software avec test préalable des nouvelles releases & fall back scénario ▪ Gestion des incidents (y compris la communication) ▪ Avoir des procédures de backup: création, test de restauration ▪ Avoir une procédure liée au cryptage des données

4.10 La sécurité des communications

Mesure de sécurité	Mesures minimales à mettre en place
Une mesure de sécurité doit prendre en compte la sécurité des transmissions de l'information afin d'éviter les accès non autorisés aux infrastructures et aux données de l'organisation, que cet accès soit volontaire ou non.	Avoir un système détaillé et maintenu, revu, des contrôles d'accès tant physiques que logiques

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
Cette mesure de sécurité devra tenir compte de l'accessibilité requise pour les systèmes de l'organisation.	Mettre en place un inventaire des flux, de leurs responsables et des accès octroyés

4.11 Acquisition, développement et maintenance des systèmes d'information

Mesure de sécurité	Mesures minimales à mettre en place
Implémentez des contrôles pour l'acquisition, le développement et la maintenance de tout nouveau système. L'aspect d'outsourcing, l'utilisation de services en nuage ou l'achat de produits nécessitent une attention particulière.	Une approche structurée placée sous la supervision d'un responsable de l'organisation devra être développée afin de gérer efficacement l'intégration, le développement, la maintenance et le décommissionnement des solutions choisies par l'organisation. Un inventaire des systèmes choisis ainsi que la référence aux contrats et obligations (SLA, NDA) sera établi par l'organisation afin d'assurer le suivi et la gestion des solutions externalisées.
De plus, chaque organisation tiendra un journal avec les différents éléments suivants:	▪ Les changements ▪ Les incidents & leurs conséquences ▪ Les accès ▪ La maintenance ▪ Les mesures de sécurité mises en place
Le journal spécifiera aussi les mesures de sécurité mises en place pour:	▪ Les mesures de continuité ▪ L'intégrité des données ▪ Le problème de confidentialité ▪ La disponibilité des systèmes ▪ Les mesures pour la gestion des incidents
L'organisation mettra en œuvre des procédures afin de maintenir ses solutions à jour et assurera une mesure de sécurité de backup testée tant pour ses systèmes que pour ses données.	

Mesure de sécurité	Mesures minimales à mettre en place
Lors de l'achat, le développement et la maintenance de systèmes, processus et procédures doivent être utilisés pour protéger les données personnelles, à la fois pendant la conception et la gestion opérationnelle	Réf. RGPD Art 25. Etablir et maintenir des processus et procédures garantissant que ▪ Les systèmes et les processus sont conçus en toute sécurité ▪ Les systèmes et les processus sont utilisés en toute sécurité (protection des données par le biais de paramètres standard)

4.12 Relations avec les fournisseurs

Mesure de sécurité	Mesures minimales à mettre en place
L'organisation s'assurera que les contrats entre parties mentionneront les mesures de sécurité imposées par l'organisation, les lois et règlements (notamment le RGPD) ainsi que les éléments de contrôle et de revue.	
Chaque organisation veillera à encadrer les relations avec les fournisseurs et les autorités.	Les contrats/documents doivent clairement fixer la répartition des obligations à respecter ainsi que les responsabilités des différentes parties.
Chaque organisation veillera à faire appel aux services de 'cloud computing' qui correspondent aux mesures de sécurité nécessaires pour l'organisation.	Basé sur une analyse des risques pour les services / données externalisées – pour ce faire, vous pouvez utiliser les rapports d'audit disponibles (ISO, ISAE3402, ENISA, SANS, CSA, etc.). Valider les rapports d'audit et les certifications des fournisseurs de services cloud

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation veillera à ce que les relations avec les fournisseurs et les autorités soient définies.	Les contrats / documents doivent clairement indiquer qui est le responsable du traitement et quelle partie est le sous-traitant et comment les responsabilités sont attribuées.
	La manière dont la protection des données est organisée, y compris la sécurité et le comportement requis, la gestion des incidents, le signalement des violations, le contact avec les autorités (ou non) doit être clairement convenue avec chaque sous-traitant.

4.13 Politique Coordonnée pour publication des vulnérabilités de sécurité

Mesure de sécurité	Mesures minimales à mettre en place
Une Politique Coordonnée pour publication des vulnérabilités ('*Coordinated Vulnerability Disclosure Policy*' – ci-dessous CVDP) **L'organisation élabore et applique une CVDP.**	La politique doit être approuvée légalement par un responsable de l'entreprise (p.ex. le directeur). Le CVDP est un ensemble de règles préalablement définies par l'organisation, responsable des technologies de l'information, et qui permettent aux chercheurs en sécurité (pirates éthiques) ou au grand public de rechercher les vulnérabilités potentielles des systèmes de cette organisation avec de bonnes intentions. ou de lui fournir toutes les informations pertinentes qu'ils découvrent à cet égard, sans faire l'objet de poursuites.
	Le contenu du CVDP doit être disponible sur votre site Web et accessible à des tiers. Si possible, le CVDP doit être écrit dans les différentes langues de votre site web. Nous vous recommandons d'écrire un texte concis mais complet, indiquant clairement:**L'applicabilité de la politique**; ▪ La portée de votre politique. ▪ Les limites de droit d'accès; ▪ La manière dont un ethical hacker **peut changer ou détruire, ou non, des données**.

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
Les employés internes et externes ainsi que les personnes impliquées doivent disposer d'une procédure permettant de signaler les activités suspectes.	Une procédure de signalement, d'enregistrement et de traitement des infractions potentielles ou présumées afin que les vulnérabilités puissent être traitées rapidement et de manière structurée.

Mesure de sécurité	Mesures minimales à mettre en place
Notification à l'autorité de contrôle d'une violation de données à caractère personnel	L'autorité de protection des données (APD) reçoit dans les 72h de la constatation la notification des brèches de sécurité concernant des données à caractère personnel

4.14 Gestion des incidents liés à la sécurité de l'information

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation mettra en place un plan de gestion des incidents qui reprendra:	Déterminer les rôles et responsabilités
	Registre interne des incidents contenant tous les incidents de sécurité signalés
	Les outils de détection (internes ou externes)
	La notification par tout employé ou partie tierce d'intrusion, d'élément suspicieux, de perte ou de destruction
	Les niveaux d'alerte – définition des critères d'escalation vers une crise
	La procédure de gestion de crise (y compris la communication)
	L'information et la formation sont nécessaires par le biais de différents canaux.
	Relié aux infrastructures IC & OES de CERT.be (collecte de renseignements / échange d'informations).

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
	Dans le respect de toute autre obligation règlementaire et/ou sectorielle (par exemple énergie, banque, télécom)
Chaque incident sera analysé afin d'évaluer la pertinence de nouvelles mesures de sécurité.	Les "lessons learned" (enseignements tirés) de chaque incident (interne et/ou externe) permettront d'améliorer la procédure de gestion des incidents pour l'organisation.
	Le signalement d'éventuels incidents de sécurité doit être rendu possible sans que les employés soient punis ou exposés à la vengeance des employés ou de leurs supérieurs hiérarchiques.

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation établit un plan de gestion des incidents comprenant les tâches et responsabilités suivantes, qui régit le traitement des violations de données à caractère personnel.	Détermination des rôles et responsabilités en cas d'incidents et de violations de données personnelles
	Registre des incidents contenant tous les incidents de sécurité des informations signalés, avec la réserve nécessaire pour pouvoir déclarer ces incidents aux autorités compétentes (APD), en raison de l'impact significatif sur les données personnelles des personnes impliquées.
	Equipé d'outils d'investigation (internes ou externes).
	Plan de communication avec les parties impliquées ▪ gestion des rapports; ▪ signaler à l'autorité; ▪ notification des personnes impliquées (si nécessaire); ▪ ...

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

Mesure de sécurité	Mesures minimales à mettre en place
Notification à l'autorité de contrôle d'une violation de données à caractère personnel	Chaque organisation signale les incidents liés aux données à caractère personnel conformément aux dispositions des articles 33 et 34 de la RGPD.

4.15 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

Mesure de sécurité	Mesures minimales à mettre en place
Pour tout système critique ou toute donnée sensible nécessaires à la continuité de l'organisation, un plan de continuité sera mis en place.	Une attention particulière sera portée aux points suivants: • Inventaire des systèmes/actifs critiques • Gestion des risques • La compétence des employés responsables des différents processus/actifs essentiels à l'organisation • Les niveaux requis de criticité pour l'activation du plan de continuité • La priorisation des actifs essentiels dans leur restauration • La gestion de la communication
Maintenance du plan de continuité	Une révision et adaptation de ce plan de continuité sont nécessaires, à l'instar d'un test/d'une simulation.
Système de protection garantissant la confidentialité, l'intégrité et la disponibilité des données personnelles et de l'entreprise	Le responsable du traitement doit s'assurer que la disponibilité et l'accès aux données de l'entreprise et aux données personnelles peuvent être restaurés à temps après un incident physique ou technique.
	Protection de la société et des données personnelles contre la perte, la modification ou la destruction non autorisée, que ce soit par accident ou par suite d'une action volontaire.

4.16

4.16 Encadrer les relations avec les tiers et les autorités

Mesure de sécurité	Mesures minimales à mettre en place
Conformité aux dispositions légales et règlementaires	Chaque organisation agira conformément aux dispositions légales et règlementaire.
Chaque organisation veillera à ce que les relations avec les fournisseurs et les autorités soient définies.	Les contrats/documents doivent indiquer clairement les responsabilités des différentes parties impliquées et la manière dont les responsabilités sont attribuées.

Mesure de sécurité	Mesures minimales à mettre en place
Suivi de la législation et des avis émis ou modifiés par les autorités compétentes.	Suivi des publications d'avis et de la législation des autorités compétentes
	Désignation d'un responsable pour garantir le suivi de la législation et des avis émis ou modifiés par les autorités compétentes.
	Contrat de traitement au sens de l'article 28 des RGPD.

4.17 Evaluation des mesures des sécurité

Mesure de sécurité	Mesures minimales à mettre en place
Chaque organisation organisera régulièrement:	Une évaluation interne ou externe sur la sécurité de l'information. Cette évaluation externe pourra être réalisée par le service Fédéral d'Audit Interne (FAI).
	Un rapport de contrôle sur la situation de la sécurité rédigé par un auditeur interne ou le conseiller en sécurité de l'information sera présenté au comité de direction
	Une évaluation ou un suivi peut être effectué à intervalles réguliers, mais il est également intéressant d'effectuer un suivi immédiatement après un incident, car il s'agit d'un indicateur utile pour atteindre un point d'amélioration.

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

5 Revue annuelle du plan de sécurité avec l'approbation de la direction

Il est conseillé de revoir ce plan de sécurité annuellement avec la direction.

Cela permettra de le corriger et de le compléter ainsi que de l'aligner avec un plan protection des données.

Le plan de sécurité de l'information est amené à évoluer dans le temps. Il pourra notamment être revu afin de prendre en compte:

- de l'es évolution des menaces et des retours d'expérience du traitement des incidents;
- des résultats d'analyses de risques ainsi que des actions découlant de contrôles ou d'audits;
- des évolutions des contextes organisationnels, juridiques, réglementaires et technologiques.

Le suivi de ces évolutions est assuré par la direction des différents SPF qui a pour principales missions:

- de suivre la mise en œuvre des plans de sécurité;
- de mesurer les progrès et l'état de la sécurité de votre organisation;
- de proposer des mises à jour;
- de proposer des documents complémentaires et des directives permettant d'en faciliter ou d'en préciser la mise en œuvre;
- de suivre les évolutions des documents techniques.

Certaines organisations sont obligées de faire rapport sur l'état d'avancement de leur plan de sécurité et le plan de protection des données (voir norme ISO 29100 et ISO29101).

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

6 Panel d'experts

Ce document a été élaboré grâce à la participation active des conseillers en sécurité et experts issus des instances suivantes:

Instance
SPF Justice
DGCC
Police Fédérale
SPF Chancellerie
SPF Santé
SPF Economie
CCB
SPF BOSA
APD

7 Acronymes & Abréviations

7.1 Terminologie (Générale)

Acronyme	Description
Les techniciens de l'information	Peuvent être définis comme toutes les personnes qui possèdent, dans le cadre de leurs responsabilités pour un système TIC, des droits d'accès qui excèdent l'usage fonctionnel des données. Il s'agit entre autres des développeurs, des gestionnaires et opérateurs systèmes, des gestionnaires de données, des développeurs et gestionnaires de logiciels, des opérateurs de réseau, des consultants et des sous-traitants.
Le conseiller en sécurité de l'information	Soutenu par le responsable de traitement promeut le respect des lois et règlements en matière de sécurité informatique. Il a une mission d'avis, de stimulation, de documentation, de contrôle et de promotion du respect des règles de sécurité imposées par une disposition légale ou règlementaire ou en vertu d'une telle disposition. Il promeut l'adoption, par les personnes employées dans l'organisation, d'un comportement favorisant la sécurité. Dans ce cadre, il est à l'évidence un partenaire privilégié de beaucoup de personnes dans l'organisation comme par exemple des gestionnaires d'information, des "data owner", des "business owners", mais aussi de beaucoup de partenaires externes, des fournisseurs, des autorités, …
Le responsable du traitement (BSG, en général)	une personne physique ou légale, un organisme gouvernemental, un service ou un autre organisme qui, seul ou avec d'autres, détermine l'objectif et les moyens du traitement des données de l'entreprise;

Acronyme	Description
Actif/Asset	Un actif est une chose ou une caractéristique matérielle ou immatérielle qui a de la valeur pour une organisation. Il existe plusieurs types des actifs. Certains d'entre eux comprennent des choses évidentes comme des machines, installations, brevets et logiciels. Mais le terme peut aussi inclure des choses moins évidentes comme les services, l'information et les gens, et des caractéristiques telles que la réputation et l'image ou la compétence et connaissance.
Actif informationnel	L'information qui a de la valeur pour une organisation.

ATTENTION
Dans le BSG, ce terme "responsable du traitement" s'applique plus largement que simplement RGPD, car il s'agit de données commerciales ET de données personnelles. **(Voir ci-dessous)**

7.2 Terminologie (RGPD)

Acronyme	Réf. RGPD	Description
Données à caractère personnel	Art. 4 1)	*"toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant"*
Traitement	Art. 4 2)	*"toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;"*
Violation de données à caractère personne	Art. 4 12)	*Une violation de la sécurité entraînant, de manière accidentelle ou illicite,* • *la destruction,* • *la perte,* • *l'altération,* • *la divulgation non autorisée* *de données à caractère personnel* • *transmises, conservées ou traitées d'une autre manière, ou* • *l'accès non autorisé à de telles données;*
Responsable du traitement sous RGPD	Art. 4 7)	*"la personne physique ou morale, l'autorité publique, le service ou un autre organisme*

CENTRE POUR
LA CYBERSECURITÉ BELGIUM
Rue Loi 18 – Bruxelles

		qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement"

7.3 Acronymes

Acronyme	Description
BCP (EN)	Business Continuity Planning
CIA (EN)	*Confidentiality, integrity and availability (EN)*
CID	Confidentialité, intégrité et disponibilité = CIA (EN)
CVDP (EN)	Coordinated Vulnerability Disclosure Policy (EN)
DGCC	Direction Générale Centre de Crise
FISP	Federal Information Security Policy (projet par BOSA)
NCCN	Nationale Crisis Center – Centre de Crise National
PCA	Plan de continuité des activités
PCPV	Politique coordonnée pour publication des vulnérabilités
PDCA (EN)	Plan, Do, Check, Act (EN)
RGPD	Règlement Général sur la Protection des Données = GDPR (EN)
GDPR (EN)	General Data Protection Regulation (EN) = RGPD (FR)

8 Références

Référence	Description & URL
RGPD	*RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement Général sur la Protection des Données)* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

CENTRE POUR

LA CYBERSECURITÉ BELGIUM

Rue Loi 18 – Bruxelles

CENTRE FOR CYBER SECURITY BELGIUM

Les informations fournies:

- sont exclusivement à caractère général et n'entendent pas prendre en considération toutes les situations particulières;
- ne sont pas nécessairement exhaustives, précises ou actualisées sur tous les points;

Editeur responsable:

CENTRE POUR LA CYBERSECURITE BELGIQUE

Rue de la Loi, 18

1000 Bruxelles