Organisation visée	Type d'informations		
Groupe Volvo, AA10000	Instructions		
Secteur Département de la protection des renseignements personnels, AA14110	Numéro du document 0001-14-27269		Catégorie d'Informations Interne
Responsable	Version	Date de révision	Page
Giraudon, Guillaume	3.0	10/6/2020	1 / 14

0001-14-27269 Procédure en cas de violation à des données personelles

Table des Matières

Le présent document a été émis par le Système de Gestion du Groupe Volvo. Veuillez-vous assurer de toujours avoir en main la version la plus récente si vous l'imprimez ou le téléchargez.

1. Définitions

Données Personnelles – Toute information relative à une personne physique spécifique ou à tout le moins identifiable, peu importe qu'elle soit structurée ou non ou se présente sous un format papier ou numérique.

Violation de Données Personnelles (VDP) – Aux dires du *Règlement général sur la protection des données* (« RGPD ») et de la *Loi sur la protection des renseignements personnels dans le secteur privé* (« LP »), toute faille de sécurité entraînant l'accès, l'altération, la perte, la destruction ou la divulgation illégale ou accidentelle de Données Personnelles et ayant pour effet d'exposer les droits et libertés d'une Personne concernée à un risque indu. En vérité, de tels droits et libertés peuvent être compromis dès que le Traitement de Données Personnelles est susceptible d'entraîner quelque forme de préjudice physique, matériel ou immatériel (tel qu'un vol d'identité, une fraude, une perte financière, une divulgation non autorisée ou l'impossibilité pour une Personne concernée de contrôler adéquatement ses Données Personnelles).

Il existe trois (3) grandes catégories de violation à des Données Personnelles :

- **[Disponibilité]** Impossibilité d'accéder à des Données Personnelles ou destruction de telles données.
  - Exemple: certaines Données Personnelles sont perdues en raison d'une panne de courant ou d'une catastrophe naturelle (incendie, inondation, etc.)
- **[Intégrité]** Altération de Données Personnelles.
  - Exemple: des informations relatives aux salaires gagnés par des employés sont confondues au cours d'une mise à niveau technique.
- **[Confidentialité]** Accès ou divulgation non autorisé(e).
  - Exemples:
    - Un courriel contenant des Données Personnelles est transmis au(x) mauvais destinataire(s);
    - Des pirates ont accès à des Données Personnelles au cours d'une cyber-attaque;
    - Un ordinateur portable contenant des Données Personnelles est perdu ou volé.

Pour sa part, une faille de sécurité dite "**personnelle**" consiste en un incident en lien avec :

- La **Sécurité des TI** (cyber-attaque, bogue détecté au sein d'une application, etc.) ou
- La **Sécurité des Informations** (exemple: une annexe contenant des Données Personnelles est transmise au mauvais département d'une organisation).

Les définitions auxquelles il est fait référence à la Directive relative aux données à caractère personnel s'appliquent au présent document, compte tenu des adaptations nécessaires.

2. Objectif et Portée

Le présent document s'applique à toutes les entités juridiques faisant partie du Groupe Volvo, de même qu'à tous les membres du personnel de cette dernière (y compris les consultant et les salariés embauchés en vertu d'un contrat à court terme) qui sont appelés à traiter des Données Personnelles dans le cadre de leurs fonctions.

Les instructions figurant au présent document tiennent compte des formalités qu'impose le RGPD et LP en matière de traitement de Violation de Données Personnelles.

Certain(e)s modèles et instructions plus détaillés s'adressant aux principales parties prenantes seront fournis plus loin.

Les obligations, devoirs et responsabilités incombant à l'entreprise en matière de Violation de Données Personnelles varieront en fonction du rôle qu'elle occupe – soit celui de Responsable de traitement ou d'Unité de Traitement.

Le présent document a été émis par le Système de Gestion du Groupe Volvo. Veuillez-vous assurer de toujours avoir en main la version la plus récente si vous l'imprimez ou le téléchargez.

3. Obligations du Groupe Volvo et de Nova Bus

Le Groupe Volvo et Nova Bus sont, en vertu de la loi, tenus de s'assurer que toutes les Violations de Données Personnelles sont détectées et traitées en temps opportun et de manière sécuritaire.

- En tant que **Responsable de traitement**, le Groupe Volvo et Nova Bus doivent :
  - **Déclarer la Violation à des Données Personnelles aux Autorités de Supervision compétentes (au Québec, la Commission d'accès d'information.)**
    - **Les VDP dont il est question au RGPD ou LP doivent être déclarées <u>dans les 72 heures</u>** qui suivent leur détection, à moins qu'une VDP particulière ne soit pas de nature à compromettre les droits et libertés de quelque personne physique.

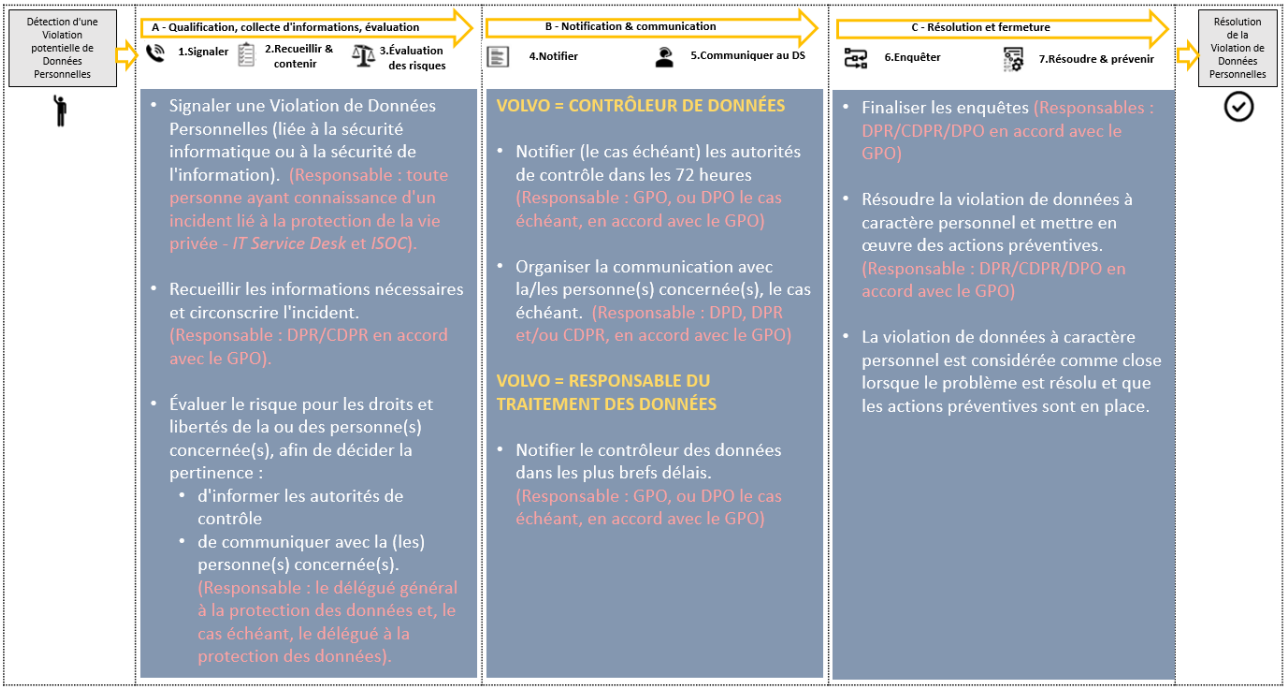
  - Dès qu'une Violation de Données Personnelles pose un risque élevé aux droits et libertés d'une ou de plusieurs personnes physiques, le Groupe Volvo **doit sans délai divulguer la situation aux Personnes concernées**.

- En tant qu'**Unité de Traitement**, le Groupe Volvo et Nova Bus doivent :
  - **Aviser sans délai le Responsable de traitement de la survenance d'une Violation de Données Personnelles.** Aucune Unité de Traitement n'a l'obligation de contacter quelque Autorité de Supervision ou Personne concernée. Elles doivent, par contre, détecter, évaluer, confiner, investiguer et résoudre la VDP tout en se conformant aux instructions du Responsable de traitement.

4. Procédure en cas de Violation de Données Personnelles

La figure ci-dessous résume les différent(e)s étapes, séquences d'activités et items livrables composant le processus en cas de Violation de Données Personnelles. Chacune des activités couvertes s'accompagne d'une courte description et d'instructions sommaires.

4.1. Survol du processus



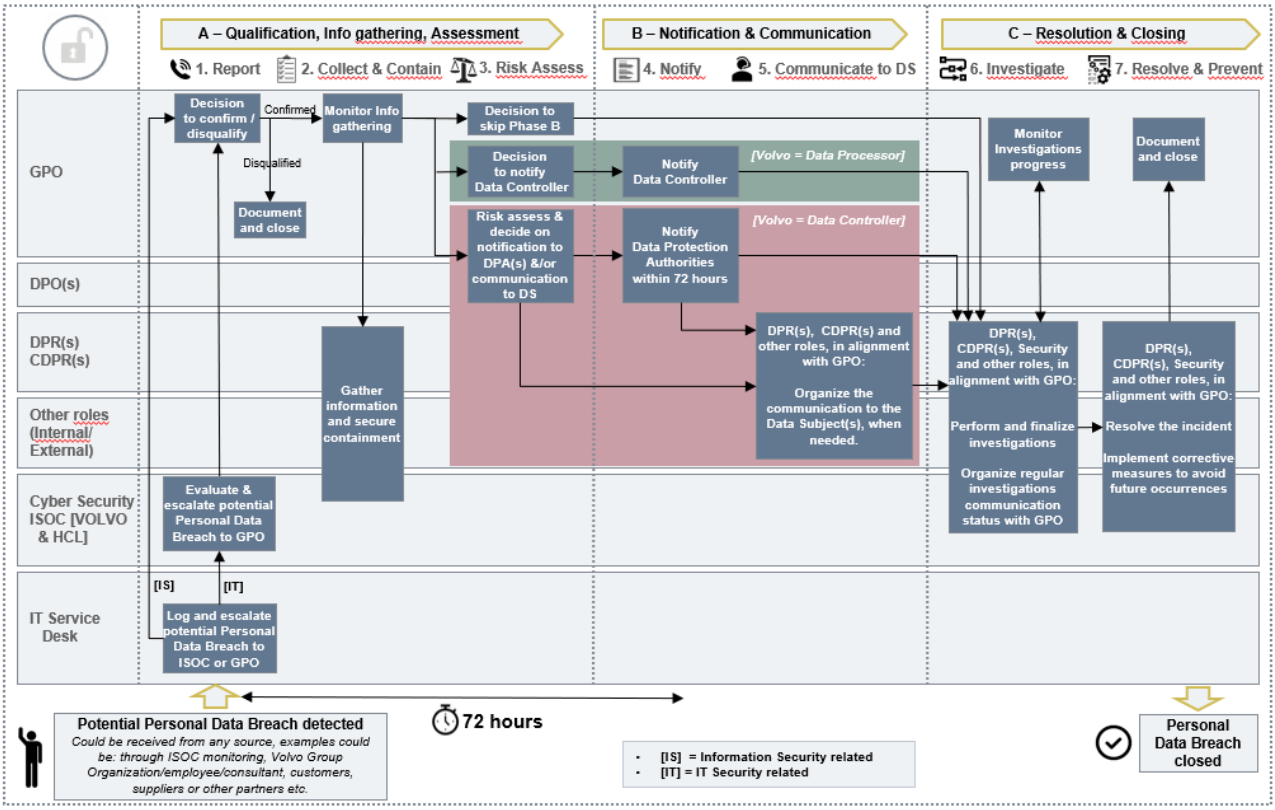
- **Déclenchement du processus:** Le processus de Traitement de Violation de Données Personnelles se déclenche dès qu'une Violation Potentielle est détectée.
- **Trois (3) principales étapes du processus:**
  - Phase A – Qualification, Cueillette d'Informations et Évaluation
  - Phase B – Déclaration et Échanges Subséquents
  - Phase C – Résolution et Clôture

- **Fin du processus:** Le processus de Traitement de Violation de Données Personnelles se termine une fois que la VDP a été convenablement documentée et résolue.

4.1.1. Exigences de Base

- Confidentialité des données: Il est crucial d'assurer la confidentialité des Données Personnelles traitées au cours du processus – notamment en ne les partageant qu'avec les parties prenantes en charge de la résolution de l'incident.
- Agir rapidement: Toutes les VDP doivent être déclarées à l'intérieur des délais prescrits (i.e., 72 heures dès que le RGPD s'applique; pour la LP, le VDP doit agir avec 'diligence'). En vue d'éviter tout délai de traitement indu, tout incident devrait être évalué le plus rapidement possible (même si certaines informations additionnelles demeurent requises).

4.2. Caractéristiques du Processus



Le présent document a été émis par le Système de Gestion du Groupe Volvo. Veuillez-vous assurer de toujours avoir en main la version la plus récente si vous l'imprimez ou le téléchargez.

4.2.1. Déclenchement du Processus: Détection d'une Violation Potentielle

Une Violation de Données Personnelles peut provenir :

- D'une source externe (i.e., étrangère au Groupe Volvo ou Nova Bus) telle qu'une personne physique ou morale (client, fournisseur, conducteur, candidat à un poste, etc.) agissant en qualité du Responsable de traitement ou d'Unité de Traitement public(que) ou privé(e). Une telle violation sera généralement déclarée par l'entremise d'un moyen de communication traditionnel tel que le téléphone, le courrier électronique ou un formulaire en ligne.
- D'une source interne (i.e., rattachée au Groupe Volvo ou Nova Bus) telle qu'un employé ou un consultant, ou encore par l'entremise de procédures de surveillance manuelles ou automatisées*.

* Volvo a mis en place certains mécanismes internes lui permettant de détecter et d'adresser toute Violation de Données Personnelles potentielle. La division "Cybersécurité" du Département TI du Groupe Volvo doit établir certaines exigences de base par l'entremise du Centre d'Assistance et du Département ISOC (qui en pratique encadre tous les aspects de l'environnement TI du Groupe – y compris les Violations de Données Personnelles)

4.2.2. Phase A – Qualification, Cueillette d'Informations et Évaluation

4.2.2.1. Étape 1: Déclaration d'une potentielle Violation de Données Personnelles

Seule façon de déclarer une violation

Toutes les Violations de Données Personnelles doivent, sans aucune exception, être déclarées au Centre d'Assistance TI. Chez Nova Bus, il faut déclarer toutes violations au responsable de la protection des renseignements personnels. Dans l'éventualité où quelque Violation Potentielle était rapportée à tout autre département, ce dernier devra la réacheminer au Centre d'Assistance TI.

Procédure d'escalade

En pratique, une Violation de Données Personnelles correspond à tout incident :

- En lien avec la **Sécurité TI**, tel que :
  - Un bogue d'application entraînant une divulgation de données à quiconque ne devrait pas les connaître;
  - Une divulgation de Données Personnelles attribuable à l'hameçonnage de courriels;
  - Une modification erronée de Données Personnelles suite à une mise à niveau technique.
- En lien avec la **Sécurité des Informations**, tel que :
  - Un courriel contenant des Données Personnelles est envoyé au(x) mauvais destinataire(s);
  - Du courrier traditionnel contenant des Données Personnelles est transmis au mauvais destinataire;
  - Des sondages sont administrés d'une façon telle que certaines Données Personnelles sont divulguées aux mauvaises personnes;
  - De l'équipement TI non protégé ou susceptible d'être déverrouillé (ordinateur, téléphone mobile…) est perdu ou volé.

Le Centre d'Assistance TI doit prendre note des incidents et les soumettre à la procédure d'escalade jusqu'à ce qu'ils atteignent soit le Département ISOC (si la Violation à des Données Personnelles concerne la **Sécurité des TI**), soit le Représentant Collectif à la Vie Privée (si la violation est plutôt en lien avec la **Sécurité des informations**).

Le Département **ISOC** confinera, investiguera et résoudra les Violations de Données Personnelles fondées sur la **Sécurité des TI**. Il devra également, en temps opportun et conformément à des principes reconnus, (i) soumettre toutes les Violations potentielles au processus d'escalade jusqu'à ce qu'elles atteignent le

Le présent document a été émis par le Système de Gestion du Groupe Volvo. Veuillez-vous assurer de toujours avoir en main la version la plus récente si vous l'imprimez ou le téléchargez.

Représentant Collectif à la Vie Privée, et (ii) fournir toutes les informations dont ce dernier et Nova Bus Inc. ont besoin en vue de réaliser une évaluation des risques.

Informations que le Centre d'Assistance doit recueillir au moment d'enregistrer l'incident

Une fois qu'ils auront été obtenus, les informations et paramètres ci-dessous aideront le Représentant Collectif à la Vie Privée à évaluer l'impact de la Violation à des Données Personnelles et à décider si oui ou non elle doit être déclarée aux Autorités Responsables de la Protection des Données.

- Description de la Violation à des Données Personnelles – *Que s'est-il passé?*
- Données Personnelles en jeu – *De quel(s) type(s) de Données Personnelles est-il question?*
- Catégories de Personnes concernées (TD) concernées – *Employés, clients, conducteurs…?*
- Pays au sein desquels se trouvent les TD – *Suède, France, Pologne…?*
- Organisations concernées – *RH, finances, GTT, fournisseurs, détaillants…?*
- Date et heure de la détection – *Quand l'incident a-t-il été découvert?*
- Date de la survenance – *Quand l'incident est-il survenu?*
- Description du contexte – *En quelles circonstances l'incident a-t-il été découvert?*

L'incident doit-il être confirmé ou ignoré?

Dès qu'une potentielle Violation de Données Personnelles lui est rapportée, le Représentant Collectif à la Vie Privée doit prendre l'une des deux décisions suivantes :

- ✓ Ignorer l'incident, auquel cas l'incident est documenté et considéré clos;
- ✓ Confirmer l'incident, auquel cas le processus de traitement se poursuit.

Le Groupe Volvo pourra estimer nécessaire de tenir une enquête succincte avant de décider si l'incident doit ou non être assimilé à une Violation de Données Personnelles.

4.2.2.2. Étape 2 : Cueillette d'informations et confinement de la Violation à des Données Personnelles

Cueillette d'informations: En vue d'évaluer convenablement la teneur et la portée de l'incident, le Représentant Collectif à la Vie Privée devra disposer de plusieurs informations essentielles, telles que (sans s'y limiter) :

- *Description de la Violation à des Données Personnelles*
- *Types de Données Personnelles à l'étude*
- *Catégories de Personnes concernées (PC) concernés*
- *Pays visés*
- *Entités juridiques concernées*
- *Départements concernés*
- *Rôle joué par le Groupe Volvo (Responsable de traitement ou Unité de Traitement)*
- *Date et heure de la détection – obligatoire*
- *Date de la survenance de l'incident*

Une liste complète des informations que doit recueillir le Représentant Collectif à la Vie Privée se trouve au document intitulé Violation de Données Personnelles – Cueillette des Informations. Pour Nova Bus, veuillez utiliser le formulaire préparé par le responsable de la protection des données personnelles.

S'il s'avère que des informations additionnelles doivent être obtenues, le Représentant Collectif à la Vie Privée doit collaborer avec le RPD/RPDP pertinent en vue d'entreprendre les activités de cueillette nécessaires. Une fois en possession de toutes les informations dont il a besoin, le Représentant Collectif à la Vie Privée doit en informer le RPD/RPDP.

Le présent document a été émis par le Système de Gestion du Groupe Volvo. Veuillez-vous assurer de toujours avoir en main la version la plus récente si vous l'imprimez ou le téléchargez.

Confinement de la Violation à des Données Personnelles: Peu importe qu'elle agisse en tant que Responsable de traitement ou Unité de Traitement, le Groupe Volvo doit prendre les mesures qui s'imposent en vue de confiner la Violation de Données Personnelles et d'en limiter l'impact sur les personnes concernées.

Les conclusions de l'évaluation réalisée par le Département ISOC doivent soutenir chacune des décisions qui sont prises en matière de confinement.

Afin de gérer et de confiner adéquatement les Violations de Données Personnelles, le Département ISOC a mis sur pied une Équipe d'Intervention en Matière de Sécurité des Informations (ci-après "EIMSI") composée de représentants de l'équipe ISOC (Volvo et HCL), du département de Cybersécurité (Volvo et HCL), du Représentant Collectif à la Vie Privée et d'autres parties prenantes. Les informations recueillies par l'EIMSI doivent être transmises au RCVP sur une base régulière. Il est de la responsabilité de l'EIMSI de gérer les aspects techniques et TI du traitement, du confinement et de la résolution de Violation de Données Personnelles.

4.2.2.3. Étape 3 : Évaluation des risques

Dès qu'il reçoit les informations dont il a besoin en regard d'une Violation de Données Personnelles dûment confirmée, le RCVP, en collaboration avec le DPD (s'il en existe un) et selon que le Groupe Volvo (ou Nova Bus) intervient en qualité que Responsable de traitement ou d'Unité de Traitement.

- **Si le Groupe Volvo (ou Nova Bus) agit en tant qu'Unité de Traitement**

Le Groupe Volvo doit, en vertu de l'article 33 du RGPD (article 3.5 alinéa 2 LP) et des dispositions de l'Entente sur le Traitement des Données conclue entre les parties, aviser sans délai le Responsable de traitement qu'elle a pris connaissance d'une Violation de Données Personnelles (ou avec diligence en vertu de LP). Il revient au Responsable de traitement de décider si les Autorités de Protection des Données et les Personnes concernées doivent être avisés de la situation.

Après avoir informé le Responsable de traitement, le Groupe Volvo (agissant en qualité d'Unité de Traitement) devrait entreprendre les activités correspondant à la phase C ("Résolution et Clôture").

- **Si Volvo (ou Nova Bus) agit en tant que Responsable de Traitement**

Le Groupe Volvo doit, en vertu de l'article 33 du RGPD (article 3.5 (2) LP), réaliser une **évaluation des risques posés par la Violation à des Données Personnelles**, et ce en considérant (d'abord et avant tout) la probabilité et l'ampleur de tout impact sur les droits et libertés des Personnes concernées.
Une telle analyse permettra d'établir:

- **S'il est nécessaire d'aviser les Autorités de Supervision**
  - Les Autorités de Supervision doivent être avisées de la situation à moins qu'il s'avère peu probable que la Violation à des Données Personnelles pose quelque risque que ce soit aux droits et libertés de Personnes concernées.
- **S'il est nécessaire d'informer les Personnes concernées**
  - Il n'est pas nécessaire d'informer les Personnes concernées de la situation à moins que la Violation à des Données Personnelles ne soit de nature à poser un risque élevé à leurs droits et libertés.

- **Risque élevé**: Un risque élevé existe lorsque la violation est susceptible de causer des dommages physiques, matériels ou immatériels (discrimination, fraude, vol d'identité, etc.) à la personne à qui les données appartiennent.

- **Probabilité:** En principe, lorsque la violation porte sur une quantité importante de Données Personnelles qui (i) révèlent la race, l'origine ethnique, l'appartenance à un syndicat ou certaines

Le présent document a été émis par le Système de Gestion du Groupe Volvo. Veuillez-vous assurer de toujours avoir en main la version la plus récente si vous l'imprimez ou le téléchargez.

opinions ou croyances politiques, religieuses ou philosophiques, (ii) comprennent des informations génétiques, relatives à l'état de santé ou à la vie sexuelle, ou se rapportant aux antécédents judiciaires ou à d'autres paramètres de sécurité, ou (iii) relèvent d'attributs personnels de la Personne concernée devant faire l'objet d'une évaluation (tels que le rendement au travail, la situation financière, l'état de santé et les intérêts et préférences personnels), le risque que des dommages physiques, matériels et/ou immatériels surviennent devrait être considéré comme probable.

Chaque fois que le RCVP et le DPD décideront d'un commun accord de n'aviser ni les Autorités de Supervision, ni les Personnes concernées, la Phase B du processus ("Déclaration et Échanges Subséquents") sera escamotée et l'on passera directement à la Phase C ("Résolution et Clôture").

Les paramètres suivants doivent être considérés au cours de toute évaluation du risque :

- Le type de violation (en termes de disponibilité, de confidentialité et d'intégrité);
- La nature la quantité et le caractère sensible des Données Personnelles (souvenez-vous que le traitement d'une petite quantité de Données Personnelles sensibles peut avoir un impact substantiel sur la Personne concernée).
- La facilité avec laquelle certaines personnes physiques peuvent être identifiées (que ce soit directement ou au moyen d'une association ou assimilation de données).
- La gravité des conséquences auxquelles certaines personnes physiques font face (en prenant pour acquis que plus les données sont de nature sensible, plus le risque posé aux droits et libertés de Personnes concernées est élevé).
- Certaines caractéristiques spécifiques aux individus concernés (personnes mineures ou vulnérables, par exemple);
- Le nombre de personne physiques concernées – quoiqu'une Violation de Données Personnelles puisse avoir un impact substantiel à l'égard d'une seule Personne concernée.
- Certaines caractéristiques propres au Responsable de traitement (par définition, Previa présente un risque élevé).
- La combinaison mathématique de la gravité d'une Violation Potentielle et de la probabilité qu'elle se produise.

L'évaluation du risque qui s'impose à l'égard de chaque Violation de Données Personnelles dûment confirmée est décrite à l'outil d'enregistrement ainsi qu'au modèle intitulé Violation de Données Personnelles – Évaluation des Risques. Pour Nova Bus, veuillez utiliser le formulaire préparé par le responsable de la protection des données personnelles.

Circonstances où il n'est pas nécessaire de procéder à une divulgation: Aucune Violation de Données Personnelles qui n'est que "très peu susceptible de compromettre sérieusement les droits et libertés de personnes physiques" ne doit être communiquée aux Autorités de Supervision – par exemple lorsque les Données Personnelles sont déjà de connaissance publique et que le fait de les divulguer n'entraîne aucun risque potentiel pour la personne physique concernée.

Un autre exemple de violation ne requérant aucune divulgation en faveur des Autorités de Supervision serait celui de la perte ou du vol d'un appareil mobile encodé qu'utilise certains membres du personnel du Groupe Volvo. Si tant est que la clé d'encodage demeure en la possession sécurisée du Groupe Volvo et qu'il existe d'autres exemplaires ou copies des Données Personnelles, la personne qui est en possession de l'appareil ne pourra accéder à ces dernières. S'il appert éventuellement que la clé d'encodage a été compromise ou que le logiciel ou l'algorithme d'encodage est vulnérable, le niveau de risque auquel font face les Personnes concernées sera mis à jour et il pourra s'avérer nécessaire de divulguer la situation.

Documentation

Le Représentant Collectif à la Vie Privée doit, par écrit et au moyen de l'outil d'enregistrement des Violations de Données Personnelles, documenter le processus d'évaluation du risque de même que la décision finale qu'il prendra en conséquence. Chez Nova Bus, la décision finale sera prise par écrit par le responsable de la

Le présent document a été émis par le Système de Gestion du Groupe Volvo. Veuillez-vous assurer de toujours avoir en main la version la plus récente si vous l'imprimez ou le téléchargez.

protection des données personnelles. Les modèles prescrits à cette fin sont inclus à la fin du présent document.

4.2.3. Phase B – Déclaration et Échanges Subséquents

Les activités dont il est question à la Phase B sont entreprises sur la foi de décisions prises au cours du processus d'évaluation des risques posés par la Violation à des Données Personnelles (Phase A, Étape 3), qui, par définition, varieront en fonction du rôle que tient le Groupe Volvo ou Nova Bus (Responsable de traitement ou Unité de Traitement).

4.2.3.1. Étape 5: Déclaration

- **<u>Si Volvo ou Nova Bus agit en tant qu'Unité de Traitement</u>**

Le Groupe Volvo doit communiquer avec le Responsable de traitement dès qu'elle prend connaissance d'une Violation de Données Personnelles – une obligation qui lui incombe déjà aux termes de l'Entente sur le Traitement des Données que les parties ont conclue.

En pareil cas, le Groupe Volvo doit (entre autres choses):

- Définir la nature de la Violation à des Données Personnelles, en précisant (si possible) les catégories et le nombre approximatif de Personnes concernées, de même que les catégories et le nombre approximatifs de dossiers personnels visés.
- Communiquer le nom et les informations de contact du Responsable de la Vie Privée, du Responsable de la Protection des Données (le cas échéant), de même que de toute autre personne-ressource susceptible de fournir des informations utiles.
- Décrire les conséquences les plus probables de la Violation à des Données Personnelles.
- Définir les mesures envisagées ou déjà prises par le Responsable de traitement en vue de confiner et de résoudre la Violation de Données Personnelles (y compris, le cas échéant, toute initiative visant à en atténuer les conséquences potentielles).

Le modèle intitulé Violation de Données Personnelles – Avis à Transmettre aux Responsables de traitement peut être utilisé en de telles circonstances. Pour Nova Bus, veuillez utiliser le formulaire préparé par le responsable de la protection des renseignements personnels.

- **<u>Si Volvo ou Nova Bus agit en tant que Responsable de traitement</u>**

Le Groupe Volvo, par l'entremise du RCVP et du DPD (s'il en existe un) devront, au plus tard soixante-douze (72) heures après en avoir pris connaissance, déclarer la Violation à des Données Personnelles aux Autorités de Supervision.

"Prendre connaissance" ou "être au fait" de quelque chose implique un niveau de certitude à tout le moins raisonnable. Une fois informé (à l'interne ou à l'externe) d'une potentielle Violation de Données Personnelles, le Groupe Volvo pourra entreprendre une enquête succincte (Phase A, Étape 1 – "L'incident doit-il être confirmé ou ignoré?") en vue de déterminer si une violation a bel et bien eu lieu. Au cours d'une telle enquête, le Groupe Volvo ne sera pas considérée être "au fait" de la situation. L'enquête initiale devrait débuter le plus rapidement possible et permettre de déterminer (avec un niveau de certitude raisonnable) si oui ou non une violation s'est produite et s'il est nécessaire de procéder à une enquête plus approfondie afin d'en évaluer les impacts potentiels.

Bien que l'autorité suédoise en matière de protection de données soit la firme *Datainspektionen*, il est possible qu'une série de facteurs spécifiques (tels que le pays de résidence de certains Personnes

Le présent document a été émis par le Système de Gestion du Groupe Volvo. Veuillez-vous assurer de toujours avoir en main la version la plus récente si vous l'imprimez ou le téléchargez.

concernées) obligent le Groupe Volvo à déclarer une Violation de Données Personnelles à d'autres Autorités de Protection des Données – par exemple CNIL, s'il appert que la violation porte sur les Données Personnelles d'employés de Renault Trucks résidant en France. Au Québec, l'autorité est la Commission d'accès à l'information.

Toutes les décisions portant sur la déclaration d'une Violation de Données Personnelles devront, d'un commun accord, être prises par le RCVP et le DPD compétents.

Toute déclaration acheminée aux Autorités de Protection de Données devrait, à tout le moins, comprendre ce qui suit:

a) Une description de la nature de la Violation à des Données Personnelles;
b) Les catégories et le nombre approximatif de Personnes concernées;
c) Les catégories et le nombre approximatif de dossiers personnels visés;
d) Les coordonnées du Représentant Collectif à la Vie Privée (lorsqu'applicable) et de toute autre personne-ressource susceptible de fournir des informations utiles;
e) Une description des conséquences les plus probables de la Violation à des Données Personnelles;
f) Une description des mesures envisagées ou déjà prises par le Groupe Volvo en vue d'adresser la Violation à des Données Personnelles – y compris toute initiative raisonnable visant à en atténuer les conséquences potentielles;
g) (Le cas échéant) un énoncé à l'effet que la violation implique des établissements se trouvant au sein d'autres États Membres où certains Personnes concernées sont susceptibles d'avoir été affectés;

Toute déclaration qui n'est pas transmise aux Autorités de Supervision à l'intérieur d'un délai de soixante-douze (72) heures doit être accompagnée des explications qui s'imposent.

S'il s'avère impossible de transmettre en même temps toutes les informations relatives à une Violation de Données Personnelles, les informations manquantes pourront être ajoutées par étapes dans les meilleurs délais possibles.

4.2.3.2. Étape 5: Divulgation en faveur des Personnes concernées

Il n'y a lieu de recourir à la présente étape que lorsque le Groupe Volvo agit en tant que Responsable de traitement et que la Violation à des Données Personnelles est susceptible de poser un risque élevé aux droits et liberté d'un ou de plusieurs Personnes concernées– auquel cas, le RCVP, le DPD, le RPD et/ou le RPDP (agissant de concert) informeront sans délai les Personnes concernées de la survenance d'une violation.

Toute divulgation transmise à un ou plusieurs Personnes concernées doit (à tout le moins), en des termes simples et clairs :

a) Définir la nature de la violation;
b) Fournir le nom et les informations de contact du Responsable de la Protection des Données et d'autres points de contact;
c) Décrire les conséquences les plus probables de la violation;
d) Décrire les mesures envisagées ou déjà prises par le Responsable de traitement en vue d'adresser la violation – y compris toute initiative raisonnable visant à en atténuer les conséquences potentielles; et
e) Fournir des conseils personnalisés permettant à certains individus de se protéger (au moyen d'un changement de mot de passe, notamment) à l'encontre de certaines conséquences préjudiciables de la violation.

Le présent document a été émis par le Système de Gestion du Groupe Volvo. Veuillez-vous assurer de toujours avoir en main la version la plus récente si vous l'imprimez ou le téléchargez.

S'il s'avère nécessaire d'atténuer un risque imminent de dommage, les Personnes concernées doivent en être informés sans délai. Si par contre il importe de mettre en place certaines mesures de protection à l'encontre de violations similaires ou récurrentes, il sera possible d'en aviser les Personnes concernées en temps opportun.

S'il appert qu'une divulgation individuelle adressée directement à chaque Personne concernée (au moyen d'une lettre transmise par la poste, d'un courriel ou d'un message texte) serait inefficace ou disproportionnée, il sera possible de procéder par voie d'une communication publique (annonce sur un site web, campagne par l'entremise de la presse écrite ou d'autres médias imprimés, etc.).

Aucune divulgation n'est requise dans les cas suivants :

- En tant que Responsable de traitement, le Groupe Volvo ou Nova Bus (i) a conçu et mis en œuvre des mesures de protection de nature technique et organisationnelles (par exemple certains mécanismes d'encodage rendant toute donnée personnelle illisible par quiconque n'est pas autorisé à en prendre connaissance), et (ii) a adopté d'autres mesures concrètes assurant que les risques élevés dont il est question au présent document ne puissent à nouveau compromettre les droits et liberté de Personnes concernées.

4.2.4. Phase C – Résolution et Clôture

4.2.4.1. Étape 6: Enquête

S'il appert qu'à ce state du processus certaines informations essentielles au traitement de la Violation à des Données Personnelles demeurent manquantes, il pourra s'avérer nécessaire de tenir une enquête plus approfondie,

Dans l'éventualité où une analyse de nature juridique était requise, il importera de déterminer quels types d'informations sont requises dans un tel contexte – une décision qui s'avérera tout particulièrement cruciale lorsque la violation est susceptible d'avoir un impact substantiel et/ou doit être déclarée aux Autorité de Protection des Données.

Il est de la responsabilité des RPD, des RPDP, du département de la Sécurité et d'autres disciplines d'entreprendre les activités en question. Toutes les mesures, initiatives et décisions qui seront prises devront être conformes aux instructions fournies par le DPD.

4.2.4.2. Étape 7: Résolution et Prévention

À ce stade du processus de traitement d'une Violation de Données Personnelles, les RPD et RPDP, le département de la Sécurité et d'autres disciplines doivent, toujours en conformité avec les directives fournies par le DPD, s'assurer que l'incident est résolu définitivement.

En vue de prévenir toute récurrence de la violation, il importe que les RPD et RPDP, le département de la Sécurité et d'autres disciplines réalisent une analyse de sa cause la plus probable et mettent en place les mesures correctrices qui s'imposent. Un rapport final de ces démarches devrait être transmis au DPD.

- Lorsque la Violation à des Données Personnelles s'apparente à une faille de Sécurité des TI, le département ISOC doit la résoudre et l'empêcher de se produire à nouveau conformément au Processus de Gestion des Incidents.
- Lorsque la Violation à des Données Personnelles s'apparente à une faille de Sécurité des Informations, le RCVP doit s'assurer qu'elle est résolue et que des mesures préventives sont mises en place afin de réduire à un minimum les risques qu'elle se produise à nouveau.

Le présent document a été émis par le Système de Gestion du Groupe Volvo. Veuillez-vous assurer de toujours avoir en main la version la plus récente si vous l'imprimez ou le téléchargez.

Une fois l'enquête terminée, le RCVP de même que certaines parties prenantes (telles que le DPD, le RPD, le RPDP et le département de la Sécurité) devraient s'attarder aux questions suivantes :

- Est-il nécessaire d'adopter d'autres actions, mesures ou initiatives en ce qui a trait aux avis devant être transmis aux Autorités de Supervision, aux Personnes concernées et/ou à d'autres tiers intéressés?
- Si tant est que des déclarations ont été transmises aux Autorités de Supervision ou à certaines Personnes concernées, quelles conséquences ont-elles engendrées du point de vue du Groupe Volvo?
- Dans quelles mesures y aurait-il lieu d'apporter des mises à jour ou d'autres changements aux processus de traitement des Données Personnelles (qu'ils soient ou non intégrés à des solutions TI) en conséquence d'une Violation de Données Personnelles confirmée ou potentielle?
- Est-il nécessaire de procéder à certaines mises à jour en vue d'assurer un traitement optimal des Données Personnelles et/ou une transmission plus efficace d'instructions ou de directives?

S'il s'avère nécessaire d'évaluer l'efficacité avec laquelle une Violation de Données Personnelles spécifique a été administrée, le RCVP pourra s'enquérir des « leçons apprises » en vue de déterminer si certaines améliorations s'imposent. Il devra, au surplus, (i) documenter les résultats de son analyse au moyen de l'outil d'enregistrement des Violations de Données Personnelles, et (ii) superviser la mise en œuvre des améliorations pertinentes.

Peu importe qu'une violation doive ou non être déclarée aux Autorités de Supervision, le Groupe Volvo doit conserver des dossiers au sujet de toutes les violations qu'elle traite – le tout au moyen de l'outil d'enregistrement de Violation de Données Personnelles accessible par l'entremise du Réseau Teamplace.

4.2.5. Fin du Processus

Toute Violation de Données Personnelles sera réputée être close lorsque l'incident aura été résolu ET que les mesures correctrices et/ou préventives qui s'imposent auront été mises en place.

5. Rôles et Responsabilités:

RÔLE	RESPONSABILITÉS
RCVP = Représentant Collectif à la Vie Privée **(Le rôle confié au RCVP est défini au SGVG)**	• Responsable de l'ensemble du processus de Traitement des Violations de Données Personnelles applicable à l'échelle du Groupe Volvo. • Responsable de l'analyse de toutes les Violations potentielles et de la décision d'en aviser ou non les Autorités de Supervision et/ou les Personnes concernées. Doit s'assurer que toutes les déclarations sont consignées aux Ententes sur la Protection des Données (EPD) en temps opportun et en collaboration avec le DPD (s'il en existe un).
DPD = Directeur de la Protection des Données **(Le rôle confié au DPD est défini au SGVG)**	• Recommande au DPD d'informer ou non les Autorités de Supervision locales au sujet d'une Violation de Données Personnelles. • Assure et coordonne la transmission des déclarations adressées aux Autorités de Protection des Données locales. • Participe aux divulgations adressées aux Personnes concernées (que le DPD estime nécessaires).
RPD = TD/BA/GF Représentant à la Protection des Données **(Le rôle confié au RPD est défini au SGVG)**	• Assure la gestion des activités de traitement de Violation de Données Personnelles (évaluation préliminaire, cueillette d'informations, divulgation auprès des Personnes concernées, adoption de mesures d'atténuation et clôture) – le tout en respect des instructions transmises par le DPD.

Le présent document a été émis par le Système de Gestion du Groupe Volvo. Veuillez-vous assurer de toujours avoir en main la version la plus récente si vous l'imprimez ou le téléchargez.

RPDP = Représentant à la Protection des Données d'un Pays **(Le rôle confié au RPDP est défini au SGVG)**	• Intervient en tant que point de contact local en charge de problématiques afférentes à la gestion de données personnelles au sein d'un pays spécifique. • Fournit de l'assistance au RCVP/DPD/RPD en matière de cueillette de données, de traduction et de transactions de portée locale
Autres rôles:	• Tout(e) autre poste, fonction, département ou discipline requis(e) dans le cadre de la gestion adéquate de Violation de Données Personnelles – conseillers juridiques locaux, représentants des RH, spécialiste des solutions TI, représentant d'Unité de Traitement de données (fournisseur, client…)
ISOC = Information Security Operations Center (Département de cybersécurité constitué auprès du Groupe Volvo et de HCL)	• Surveille et contrôle l'environnement TI au sein duquel le Groupe Volvo évolue. • Identifie et achemine (par voie d'escalade) jusqu'au DPD tous les incidents susceptibles d'être assimilés à une Violation de Données Personnelles. Confine, analyse et résout les Violations de Données Personnelles en adoptant une approche technique.
Centre d'Assistance TI	• Achemine (par voie d'escalade) les Violations de Données Personnelles potentielles jusqu'au département ISOC (lorsque le problème relève de la Sécurité des TI) ou jusqu'au RCVP (lorsque le problème relève de la Sécurité des Informations). Le Centre d'Assistance est administré par HCL.

6. Liste des modèles utilisés

Liens permettant d'accéder aux modèles:

- Violation de Données Personnelles – Cueillette d'informations (Veuillez utiliser le formulaire du responsable de la protection des données personnelles.)
- Violation de Données Personnelles – Évaluation des risques (Veuillez utiliser le formulaire du responsable de al protection des données personnelles.)
- Violation de Données Personnelles – Informations à transmettre au(x) fournisseur(s)
- Violation de Données Personnelles – Avis à transmettre aux Responsables de traitement

7. Liste des annexes

Les annexes suivantes ont été publiées au soutien du présent document :

- ANNEXE A : Liste de Contrôle destinée au Représentant Collectif à la Vie Privée

8. Références

- Directive relative aux données à caractère personnelle

9. Historique des versions

Date	Description des changements apportés
2020-10-07	Première publication

Le présent document a été émis par le Système de Gestion du Groupe Volvo. Veuillez-vous assurer de toujours avoir en main la version la plus récente si vous l'imprimez ou le téléchargez.

Le présent document a été émis par le Système de Gestion du Groupe Volvo. Veuillez-vous assurer de toujours avoir en main la version la plus récente si vous l'imprimez ou le téléchargez.