Guide de mise en œuvre de la nouvelle loi sur la protection des données

Janvier 2024

Éditeur :
Fondation Zewo

Les auteures :
Bernadett Gal
Martina Ziegerer

Conseils juridiques :
Martin Steiger

Impressum et contact
Fondation Zewo
Pfingstweidstrasse 10
8005 Zurich
info@zewo.ch
zewo.ch
+41 44 366 99 55

Contenu

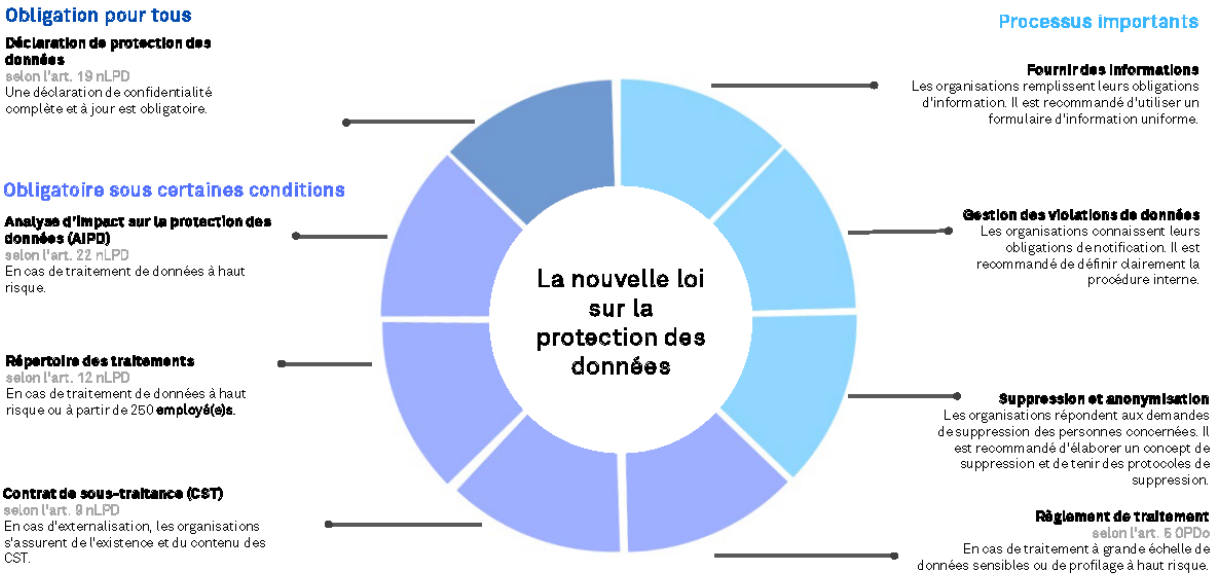
Protection des données - comment les NPO mettent en œuvre la nouvelle loi

Que doivent faire les œuvres de bienfaisance pour respecter la nouvelle loi sur la protection des données ? Cette guide à la mise en œuvre de la fondation Zewo informe qui doit établir quels documents. Les NPO reçoivent des conseils pratiques sur la meilleure manière de procéder et apprennent ce que la Zewo exigera à l'avenir en matière de protection des données.

La loi révisée protège la personnalité et les droits fondamentaux des personnes physiques dont les données personnelles sont collectées et traitées par votre organisation. La nouvelle loi sur la protection des données (nLPD) et l'ordonnance y afférente s'appliqueront à partir du 1er septembre 2023 sans période de transition.

En cliquant sur les liens suivants vous trouverez la loi révisée sur la protection des données et l'ordonnance correspondante (OLPD). En outre, l'Office fédéral de la justice (OFJ) a publié le 1er février 2023 une foire aux questions (FAQ) utile concernant la loi révisée sur la protection des données.

Cette guide à la mise en œuvre permet aux organismes d'entraide d'identifier rapidement et facilement ce à quoi ils sont concrètement tenus et quelles dispositions ils doivent prendre. Elle suit les documents et les processus régis par la nouvelle loi mentionnés ci-dessous.



Ce que Zewo exige des NPO certifiées

La norme 19 de Zewo "Protection des données" a été révisé et adapté à la modification de la loi.

Les nouvelles dispositions de la norme ne vont pas au-delà des exigences légales. La norme reprend plutôt les dispositions légales qui sont particulièrement importantes en ce qui concerne les donateurs. Lors de la première certification et de la re-certification, Zewo vérifie si l'organisation respecte la norme 19. Les prescriptions de la norme qui vont aujourd'hui déjà au-delà des exigences légales minimales restent valables.

Ces principes sont ancrés dans la norme 19 de Zewo

L'organisation respecte la protection des données et la vie privée des personnes physiques concernées, en particulier des donateurs.
Norme Zewo 19 alinéa 1

Les organisations respectent la loi applicable et actuelle sur la protection des données. Elles connaissent notamment leurs obligations d'information et de documentation et respectent les droits des personnes concernées. Les données personnelles ne sont collectées que si elles sont nécessaires aux fins de l'organisation, avec parcimonie et dans la mesure nécessaire.
Norme Zewo 19 alinéa 2

Ce qui est important pour la protection des données

La nouvelle loi vise à créer une compréhension uniforme de ce qui est actuellement important pour la protection des données en général. Elle veut sensibiliser les organisations ainsi que leurs collaborateurs et partenaires à agir de manière transparente, à veiller aux droits de la personnalité des personnes physiques, à les respecter et à sécuriser les données. Les organisations doivent identifier, analyser et, si nécessaire, optimiser les processus, systèmes, structures et contrats par lesquels elles collectent, gèrent ou traitent d'une autre manière les données des personnes physiques. L'effort organisationnel dans le domaine de la protection des données doit être adapté à la taille et aux structures des organisations concernées, ainsi qu'au type et à la quantité de traitement des données. En ce qui concerne les besoins de mise en œuvre des organisations, il existe des différences considérables.

Pour mettre en œuvre la loi révisée sur la protection des données, les œuvres de bienfaisance devraient accorder l'attention nécessaire à la protection des données. Cela signifie : mettre à disposition les capacités nécessaires et créer une compréhension interne pour ce thème.

Une déclaration de protection des données à jour - un must pour tous

Norme légale Art. 19 et suivants nLPD

Une déclaration de protection des données à jour est indispensable pour toutes les organisations, car elle constitue une partie de leur devoir d'information. Une déclaration de protection des données contribue à un traitement plus transparent des données et permet aux personnes concernées d'exercer leurs droits. La déclaration de protection des données vous permet de déclarer quelles données vous collectez auprès des personnes physiques et dans quel but. Vérifiez donc votre déclaration de protection des données existante et mettez-la à jour si nécessaire. Avant la révision de la loi sur la protection des données, la norme19 exigeait déjà une déclaration de protection des données claire, visible, facile à consulter et à jour.

Ces contenus doivent figurer dans la déclaration de confidentialité

La déclaration de protection des données indique qui collecte quelles données et pourquoi. Elle indique les personnes au sujet desquelles votre organisation collecte des données et la manière dont elle les traite. La loi exige que les déclarations de protection des données contiennent au moins les éléments suivants :

- L'identité et les coordonnées de l'organisation responsable
- Les finalités pour lesquelles votre organisation collecte et traite les données
- Les éventuels destinataires des données collectées
- Exportation éventuelle des données à l'étranger
- Les eventuelles décisions individuelles automatisées

D'autres informations possibles sont des informations sur :

- Les catégories de données personnelles collectées
- Le cercle des personnes concernées
- Les droits des personnes concernées et le lieu où elles peuvent les faire valoir
- L'utilisation de cookies, de tracking et d'autres technologies
- La démarche de l'organisation pour assurer la sécurité des données

Voici ce qu'exige la Zewo en matière de déclaration de protection des données

Les organisations collectant des dons disposent d'une déclaration de protection des données claire, bien visible, facile à consulter et à jour sur leur site web. La déclaration de protection des données est conforme aux exigences légales. Elle informe notamment sur les données personnelles qui sont collectées et traitées et à quelles fins.

En outre, la déclaration de protection des données mentionne le nom de l'organisation collectant les dons ainsi qu'une adresse de contact à laquelle les personnes concernées peuvent s'adresser pour les questions relatives à la protection des données. La déclaration de protection des données règle en outre l'éventuelle communication de données personnelles à l'étranger et les droits des personnes concernées.
Norme Zewo 19 alinéa 5

Conseils de la Zewo

Placez la déclaration de confidentialité de manière facilement accessible sur votre site web, idéalement dans le pied de page, et indiquez-la clairement. Mettez à jour la déclaration de confidentialité de votre organisation au moins une fois par an.

Vous pouvez obtenir de l'aide ici

- Vous trouverez un modèle de déclaration de protection des données via l'outil d'évaluation de la protection des données Self Assessment Tool (DSAT) ou sur le site web de ProFonds.
- **Remarque** : des conseillers juridiques, comme Datenschutzpartner AG, élaborent et actualisent votre déclaration de protection des données à l'aide du générateur de protection des données payant. Profitez du rabais que Datenschutzpartner AG accorde aux œuvres de bienfaisance certifiées Zewo. Vous trouverez votre rabais Zewo sous le lien suivant.

Analyse d'impact relative à la protection des données personnelles (AIPD)

Norme légale Art. 22 nLPD

Qui a besoin d'une analyse d'impact relative à la protection des données ?

Les organisations dont le traitement prévu de données à caractère personnel est susceptible d'engendrer un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées.

Qu'est-ce qu'une analyse d'impact relative à la protection des données ?

L'analyse d'impact relative à la protection des données est un outil de gestion des risques qui est utilisé pour déterminer si le traitement prévu de données à caractère personnel présente un risque élevé pour la personnalité ou les droits fondamentaux des personnes physiques concernées. Elle doit être élaborée avant tout traitement de données prévu, à titre de prévention des risques.

Un **risque élevé** peut résulter de la nature, de l'étendue, des circonstances, de la finalité du traitement des données ainsi que de l'utilisation de nouvelles technologies. Un risque élevé lié au traitement des données existe en grande partie lorsque des données personnelles sensibles sont traitées.

Les **données personnelles sensibles sont** les informations relatives aux aspects de la personnalité des personnes physiques, comme les données relatives aux convictions religieuses ou philosophiques, à l'orientation sexuelle, aux opinions politiques ou encore **aux données relatives à la santé.**

➔ ***Un exemple pratique :*** *un foyer pour personnes handicapées qui fournit des médicaments à ses résidents ou qui effectue d'autres traitements médicaux a besoin, traite et enregistre à cet effet les antécédents médicaux ou les données relatives à la santé des résidents. Dans ce cas, l'organisation traite des données personnelles à haut risque, car les données relatives à la santé sont des données personnelles sensibles.*

En quoi consiste une analyse d'impact relative à la protection des données ?

Les organisations doivent toujours évaluer au cas par cas les risques potentiellement élevés de leur traitement de données. Elles le font dans le cadre de leurs analyses d'impact sur la protection des données. Grâce à l'analyse d'impact relative à la protection des données, les organisations identifient à l'avance les risques potentiellement élevés pour les personnes concernées que peut comporter le traitement de données qu'elles prévoient. Les organisations définissent et contrôlent les mesures appropriées pour garantir la sécurité des données personnelles.

Si les organisations reconnaissent, grâce à leurs analyses d'impact sur la protection des données et malgré des contre-mesures définies, des risques qui pourraient entraîner des conséquences négatives indésirables de leur traitement de données, elles font appel à un soutien spécialisé.

Ce qu'exige Zewo en matière d'analyse d'impact relative à la protection des données

Les principes énoncés dans l'introduction de la **norme Zewo 19, paragraphe 2, sont appliqués**. Les exigences de Zewo ne vont pas au-delà des conditions-cadres légales. Zewo n'exige une Analyse d'impact relative à la protection des données que des organisations qui y sont légalement tenues.

Grâce à l'Analyse d'impact relative à la protection des données, les organisations identifient les risques potentiellement élevés de leur traitement de données prévu, les évaluent et définissent des mesures pour éviter les violations potentielles de la protection des données si leur traitement prévu présente des risques élevés.

Conseils de Zewo

Zewo conseille aux organisations certifiées qui sont légalement tenues d'effectuer une Analyse d'impact relative à la protection des données d'établir, en fonction des risques et avec un effort raisonnable, un processus pour l'élaboration d'analyses d'impact sur la protection des données, de les mettre par écrit et de régler les compétences personnelles. Il est en outre conseillé de tenir compte des points suivants dans une analyse d'impact relative à la protection des données :

- Description du traitement de données envisagé
- Élaboration d'une analyse des risques
- Identification de facteurs de risque particuliers
- Évaluation des risques en fonction de la gravité et de la probabilité d'occurrence
- Les mesures possibles pour faire face aux risques potentiels

Vous trouverez ici un soutien

Les documents de base « Merkblatt Datenschutz-Folgenabschätzung (DSFA) » et « Formular Datenschutz-Folgenabschätzung (DSFA) » des commissaires à la protection des données du canton de Zurich offrent par exemple une aide possible pour l'élaboration d'une analyse d'impact relative à la protection des données. Ces documents peuvent être trouvés sous ce lien. Les indications sur le contenu offrent une orientation utile pour la conception d'une DSFA.

Tenue d'un registre des traitements

Norme légale Art. 12 nLPD

Qui a besoin d'un registre des données personnelles traitées ?

Organisations qui emploient 250 personnes ou plus et/ou organisations dont le traitement des données présente des risques élevés pour les personnes concernées.

Qu'est-ce qu'un registre de traitement ?

Les organisations ainsi que leurs sous-traitants sont tenues par la loi de tenir un registre de leurs activités de traitement. Le registre de traitement ne doit pas être une liste concrète de traitements de données individuels, mais une description générale de l'activité de traitement d'une organisation. Un tel registre est également appelé inventaire des données. Les organisations sont **dispensées** de tenir un registre si elles emploient moins de 250 personnes, si elles ne traitent pas de données personnelles sensibles à grande échelle et si elles n'effectuent pas de profilage présentant un risque élevé.

A quoi sert l'inventaire : grâce à l'inventaire des données, vous obtenez une vue d'ensemble des endroits où les données des personnes physiques sont collectées, traitées ou enregistrées au sein de votre organisation. Vous pouvez passer en revue les cas les plus importants, les optimiser et les documenter.

Ce que contient l'inventaire : Il recense les domaines, processus et contextes de votre organisation dans lesquels des données de personnes physiques sont collectées, traitées ou collectées.

C'est ce à quoi vous devez veiller lors de l'établissement de l'inventaire : Il est conseillé d'établir un inventaire normalisé et systématique. Documentez et justifiez la possession et le traitement des données.

Pensez à différents groupes de personnes, comme par exemple : Collaborateurs, mandataires, bénéficiaires de prestations, donateurs potentiels, actuels ou anciens, bénévoles ou sympathisants.

Désignez les responsables de chaque domaine ou processus.

Vous trouverez ici un soutien

Vous trouverez une aide ici, sur le site de l'outil d'auto-évaluation de la protection des données DSAT. Le document « Inventaire - Aperçu des traitements de données » offre un modèle utile.

Ce que Zewo exige en matière de registre de traitement

Les principes énoncés dans l'introduction de la **norme Zewo 19, paragraphe 2, sont appliqués**. Les exigences de Zewo ne vont pas au-delà du cadre légal. Zewo n'exige un registre de traitement que des organisations qui y sont légalement tenues.

Conseils de Zewo

Zewo conseille également aux autres organisations certifiées de se pencher sur le sujet sur une base volontaire et avec un effort raisonnable, afin d'obtenir une vue d'ensemble des données traitées dans l'organisation. En effet, sans inventaire des données, il n'est guère possible de respecter la législation sur la protection des données. DSAT met à disposition un formulaire préétabli intitulé « Inventaire - traitement des données (pour les responsables) ».

Contrat de sous-traitance

Norme légale Art. 9 nLPD

Conformément à la loi (art. 9 nLPD), le traitement de données personnelles peut être confié à des sous-traitants. Il existe par exemple des rapports de sous-traitance pour : Hébergement, sauvegarde dans le nuage, apps comme Microsoft 365, comptabilité financière et salariale, services d'hébergement et de centre de données, analyses et enrichissement des données, comparaison d'adresses de tiers, agences de publicité et de collecte de fonds, lettershops ainsi qu'en cas de suivi sur différentes plateformes numériques et de traitement ultérieur des données.

Même si le traitement des données est délégué à des tiers, l'organisation qui a donné le mandat reste responsable de la protection des données. Les contrats de sous-traitance garantissent l'externalisation.

Ce que Zewo exige en matière de contrat de sous-traitance

Zewo exige des organisations certifiées qui travaillent avec des sous-traitants qu'elles vérifient leurs contrats avec de tels tiers. Concrètement, cela signifie que les organisations garantissent un traitement sûr et adéquat de leurs données par des tiers. Elles le font avant tout en choisissant et en instruisant soigneusement leurs sous-traitants, en concluant un contrat de sous-traitance approprié et en vérifiant les mesures techniques et organisationnelles visant à garantir la sécurité des données du tiers qui les traite.
Norme Zewo 19 alinéa 7

Conseils de Zewo

Zewo conseille aux organisations certifiées d'analyser systématiquement leurs contrats avec des sous-traitants afin de vérifier si la sécurité des données peut être garantie sur le plan technique et sur le plan du contenu. Les mesures techniques et organisationnelles adéquates pour la préservation de la sécurité des données sont décrites plus

précisément à l'art. 3 OLPD. Enfin, Zewo conseille aux organisations de choisir et d'instruire soigneusement leurs sous-traitants.

Remarque

Dans ce contexte, il convient de veiller à ce qu'il n'y ait pas de transfert de données à l'étranger dans le cadre du traitement par des tiers. Une liste des États à l'étranger dont la législation garantit une protection adéquate des données est établie à l'annexe 1 de l'ordonnance sur la protection des données, OPD. Cette liste est revue et adaptée périodiquement. Les organisations qui confient le traitement de leurs données à des tiers ayant leur siège à l'étranger devraient consulter régulièrement cette liste.

Règlement de traitement

Norme légale Art. 5 OLPD (Ordonnance sur la protection des données)

Qui doit établir un règlement de traitement ?

Les organisations qui traitent un grand nombre de données personnelles sensibles ou qui effectuent un profilage à haut risque.

L'obligation d'établir un règlement de traitement n'est pas inscrite dans la loi, mais dans une ordonnance. Conformément aux dispositions de l'ordonnance, les responsables, et donc les organisations ainsi que leurs sous-traitants, doivent établir un règlement de traitement automatisé lorsqu'ils établissent un **profilage à haut risque** ou traitent à grande échelle **des données personnelles sensibles**. Le règlement de traitement doit servir de manuel pour un traitement automatisé des données et contribuer à promouvoir la responsabilité des organisations.

Qu'est-ce que le « profilage » et le « profilage à haut risque » ?

Le terme « profilage » désigne tout type de traitement automatisé de données à caractère personnel permettant d'analyser certains aspects de la personnalité d'une personne physique. Les aspects de la personnalité d'une personne physique comprennent, par exemple, des informations sur sa santé, ses préférences et intérêts personnels, sa situation économique et ses lieux de résidence. Le « profilage » permet donc d'évaluer ou de juger une personne. Une telle évaluation peut porter sur des caractéristiques existantes de la personnalité d'une personne ou servir de prédiction pour des comportements futurs. Le « profilage à haut risque » présente un risque élevé pour la personnalité ou les droits fondamentaux des personnes physiques concernées, dans la mesure où le traitement des données conduit à la mise en relation d'un grand nombre de données qui permettent d'évaluer des aspects **essentiels** de la personnalité. Les aspects essentiels de la personnalité incluent par exemple les relations ou les

activités extraprofessionnelles, les convictions philosophiques ou les habitudes de consommation. La pertinence pratique de la disposition relative au profilage à haut risque reste à démontrer.

Exigences légales minimales

L'article 5 du RGPD énonce les exigences légales minimales auxquelles doit répondre le règlement de traitement. Les exigences minimales comprennent entre autres des indications sur le but du traitement, la catégorie de personnes concernées et la durée de conservation des données personnelles. Pour l'énumération exhaustive des exigences minimales en matière de contenu, les organisations concernées doivent consulter l'ordonnance mentionnée. Zewo exige des organisations certifiées qu'elles connaissent leurs obligations légales et agissent en conséquence.

Voici ce que demande Zewo concernant le règlement de traitement

Les principes énoncés en introduction dans la **norme Zewo 19, paragraphes 1 et 2, sont appliqués**. Les exigences de Zewo ne vont pas au-delà des conditions-cadres légales. Zewo n'exige un règlement de traitement que des organisations qui y sont légalement tenues.

Conseils de Zewo

Les organisations ont tout intérêt, si elles doivent établir un règlement de traitement, à l'actualiser régulièrement, à former leurs collaborateurs et partenaires sur le traitement des données personnelles sensibles et à renoncer autant que possible au profilage à haut risque.

Il est en outre conseillé de mettre par écrit le processus d'élaboration et d'actualisation du règlement de traitement et de définir clairement les responsabilités.

Processus importants

Fournir des renseignements

La loi sur la protection des données accorde entre autres aux personnes physiques concernées le droit d'être informées. Les personnes concernées peuvent donc exiger des organisations qu'elles leur indiquent si des données personnelles les concernant sont traitées. L'article 25 de la nLPD précise quelles

informations doivent être fournies. Il s'agit par exemple de l'identité et des coordonnées des responsables, des données personnelles traitées en tant que telles et du but du traitement.

Cette liste n'a pas la prétention d'être exhaustive. Pour une liste exhaustive des exigences légales minimales, il convient de consulter l'article de loi mentionné. Le législateur ne prescrit pas l'utilisation d'un formulaire de renseignements uniforme. En règle générale, les renseignements doivent être fournis par écrit, mais peuvent également l'être par voie électronique. Les renseignements volontairement faux ou incomplets sont passibles d'une amende.

Voici ce qu'exige Zewo en matière de fourniture de renseignements

Les principes énoncés en introduction dans la **norme Zewo 19, paragraphes 1 et 2, sont appliqués**. Les exigences de Zewo ne vont pas au-delà du cadre légal.

Conseils de Zewo

Zewo conseille aux organisations de définir clairement leurs processus internes, y compris les responsabilités et les compétences, dans le traitement des demandes de renseignements. Les éventuelles demandes de renseignements doivent pouvoir être traitées le plus rapidement possible et de manière compétente. La réponse aux demandes des personnes concernées doit en règle générale être fournie dans un délai de 30 jours et sans frais. Si ce délai ne peut pas être respecté, l'organisation en informe les demandeurs et fixe un nouveau délai.

Zewo recommande aux organisations certifiées d'établir un **formulaire de renseignements standardisé** afin d'uniformiser la fourniture de renseignements et d'établir des processus internes efficaces. Outre le formulaire de renseignements standardisé, il est conseillé d'établir une procédure uniforme pour l'obtention des informations. La **preuve de l'identité** de la personne qui fait la demande. Si une organisation ne traite pas les données personnelles du demandeur, elle peut néanmoins établir un renseignement négatif selon son appréciation et ses ressources.

Enfin, Zewo recommande de désigner une personne au sein de l'organisation qui sera responsable de la protection des données. La personne chargée de la protection des données devrait acquérir des connaissances de base en matière de droit de la protection des données à partir de sources publiques et être l'interlocuteur au sein de l'organisation pour les questions techniques.

Gestion des violations de données

Dans certains cas, les violations de la protection des données à caractère personnel, appelées pannes de données, doivent être notifiées au Préposé fédéral à la protection des données et à la transparence (PFPDT). Les violations de données peuvent par exemple résulter d'une destruction accidentelle ou illicite, d'une perte, d'une modification, d'une divulgation non autorisée ou d'un accès non autorisé à des données personnelles.

Des exemples pratiques de violations de la sécurité des données sont les cas de « piratage », la perte de supports de données sans cryptage adéquat ou l'envoi de courriels à divers destinataires avec des destinataires involontaires dans le CC.

Il est possible de renoncer à une notification au PFPDT si la violation de la protection des données à caractère personnel n'est pas susceptible d'entraîner un risque pour les droits et la liberté des personnes physiques concernées. Une notification doit être effectuée le plus rapidement possible après avoir pris connaissance de la violation de la sécurité des données. Les personnes concernées doivent également être informées de la violation de la sécurité des données si cela est nécessaire pour leur protection ou si le PFPDT l'exige.

Cela signifie pour les organisations que si elles enregistrent une violation de données malgré des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données personnelles (c'est-à-dire le stockage des données, l'accessibilité, la protection contre l'effacement non autorisé, etc.), elles doivent assumer leur obligation de notification. Celle-ci existe lorsque la violation de la protection des données à caractère personnel est susceptible d'entraîner un risque pour les droits et la liberté des personnes physiques concernées.

Voici ce qu'exige Zewo en matière de gestion des pannes de données

Les principes énoncés dans l'introduction de la **norme Zewo 19, paragraphes 1** et **2, sont appliqués**. Dans ce contexte, il est en outre fait référence à la **norme 19, paragraphe 6**.

L'organisation prend les mesures techniques et organisationnelles appropriées pour garantir la sécurité des données personnelles (c'est-à-dire le stockage des données, l'accessibilité, la protection contre la suppression non autorisée). Si la sécurité des données devait être violée, l'organisation assume ses éventuelles obligations de notification et d'information.
Norme Zewo 19 alinéa 6

Les exigences de Zewo ne vont pas au-delà du cadre légal.

Conseils de Zewo

Les risques potentiels doivent être évalués en fonction de la gravité des dommages potentiels et de leur probabilité d'occurrence. Si un risque potentiellement élevé ne peut pas être totalement exclu, il est conseillé de signaler la violation de données par mesure de sécurité.

Il est conseillé aux organisations de définir une procédure standardisée à suivre en cas de violation de données et d'établir ainsi une procédure de notification interne.

Remarques

Les violations de la sécurité des données peuvent être signalées ici au PFPDT.

L'objectif des mesures techniques et organisationnelles (MTO) est de garantir la sécurité des données. Avant tout, les MTD doivent rendre les données accessibles uniquement aux personnes autorisées, garantir la disponibilité des données et préserver l'intégrité des données contre toute modification non autorisée ou involontaire.

En outre, les TOM doivent permettre la traçabilité du traitement des données. L'article 3 du RGPD donne des informations détaillées sur la conception et les exigences des TOM. La bonne nouvelle, c'est que la plupart des organisations disposent déjà de TOM.

Effacement et/ou anonymisation des données personnelles

L'article 6, alinéa 4 de la nLPD stipule que les données personnelles doivent être soit détruites, soit rendues anonymes dès que leur finalité de traitement n'existe plus. Les personnes concernées peuvent exercer leurs droits à l'effacement et demander aux organisations d'effacer leurs données. Selon la loi, l'anonymisation équivaut à l'effacement. La loi exige en principe que les données personnelles soient effacées dès qu'elles ne sont plus nécessaires à leur finalité initiale. Il existe toutefois deux exceptions à l'obligation d'effacement :

Les exceptions sont les suivantes : des fins de preuve et d'autres intérêts essentiellement privés, par exemple pour la documentation ou la préservation du savoir-faire**, ou** des obligations légales de conservation. Par conséquent, il n'existe pas d'obligation absolue de suppression, mais les droits des personnes concernées sont mis en balance avec les obligations légales de conservation et les intérêts de l'organisation responsable du fichier.

Pour les organisations, cela signifie qu'elles respectent les principes de nécessité et de finalité de la protection des données. Elles collectent les données personnelles avec parcimonie et uniquement si elles sont nécessaires aux fins de l'organisation.

En outre, les organisations devraient connaître leurs obligations en matière d'effacement ou d'anonymisation des données personnelles et respecter les droits des personnes concernées en accédant à leur demande d'effacement, sauf exception à l'obligation d'effacement.

C'est ce qu'exige Zewo concernant la suppression et/ou anonymisation des données personnelles

Les principes énoncés en introduction dans la **norme Zewo 19, paragraphes 1** et **2, sont appliqués**. Les exigences de Zewo ne vont pas au-delà du cadre légal.

Conseils de Zewo

Zewo conseille aux organisations d'établir un concept de suppression interne dans le cadre de leurs ressources et après avoir évalué les risques éventuels. En outre, il peut être conseillé aux organisations de connaître le processus d'effacement de leurs processeurs de données externes. Zewo recommande en outre de tenir un protocole de suppression afin de prouver que les demandes de suppression des personnes concernées ont été satisfaites.

Enfin, les organisations feraient bien de traiter la protection des données comme un processus continu, centré sur la « gestion de la protection des données », et donc de revoir périodiquement leurs processus, documents et règlements et de les adapter si nécessaire.

Les présentes dispositions de Zewo relatives à la protection des données s'appliquent restent en vigueur

Voici ce que Zewo continue d'exiger dans la norme 19 sur la protection des données

Les organisations ne peuvent ni vendre, ni louer, ni échanger des données et des adresses collectées sur des personnes physiques, en particulier sur des donateurs et des donatrices, mais aussi sur d'autres groupes de personnes, tels que les membres, les collaborateurs, les bénévoles, les bénéficiaires de prestations, les proches, les personnes intéressées ou d'autres personnes concernées au sens de la loi sur la protection des données.

Vous pouvez utiliser de nouvelles adresses de sociétés de fourniture d'adresses en respectant le cadre légal. Ils en informent la personne concernée de manière appropriée au plus tard un mois après l'avoir reçue. Ils le font par exemple en renvoyant à leur déclaration de protection des données.
Norme Zewo 19 alinéa 3

Si des personnes souhaitent ne pas être contactées plus ou moins souvent, les organisations collectant des dons en tiennent compte et mettent cela en œuvre rapidement et sans obstacles. Cela vaut également, dans la mesure du possible, pour les premiers contacts (p. ex. prise en compte de la liste Robinson de l'Association suisse de marketing de dialogue).
Norme Zewo 19 alinéa 4

Résumé des documents obligatoires

Afin d'évaluer leurs besoins de mise en œuvre par rapport à la modification de la loi sur la protection des données, les organisations certifiées peuvent se poser les questions suivantes :

- Traite-t-on des données personnelles de personnes physiques ?
- Avons-nous 250 collaborateurs ou plus ou notre traitement de données présente-t-il un risque élevé pour les personnes concernées ?
- Le traitement de données que nous prévoyons comporte-t-il un risque élevé pour la personnalité ou les droits fondamentaux de la personne physique concernée, parce que nous traitons des données personnelles sensibles ou en raison de la nature du traitement des données ?
- Est-ce que nous traitons de manière automatisée et à grande échelle des données personnelles sensibles ou est-ce que nous réalisons un profilage à haut risque ?
- Est-ce que nous faisons traiter des données par des tiers, éventuellement à l'étranger ?

Sur la base des questions ci-dessus, il est donc possible de déterminer quels documents légaux les organisations doivent établir et dans quels cas.

Vous trouverez ci-dessous quelques exemples de documents légalement obligatoires à établir et à quel moment. Les documents et processus décrits au chapitre 2 « Quatre documents et processus recommandés » ne sont pas des documents légalement obligatoires pour tous les responsables. Le principe de proportionnalité s'applique toujours à eux. Les organisations doivent mettre en balance les risques potentiels et leurs propres ressources internes.

Exemple 1

Y a-t-il un traitement des données personnelles ?	☑	document requis	***Oui***	***Déclaration de confidentialité***
Y a-t-il 250 collaborateurs ou plus ou des données à haut risque sont-elles traitées ?	☒	document requis	*Non*	Registre de traitement
Le traitement de données prévu présente-t-il un risque élevé ?	☒	document requis	*Non*	Analyse d'impact relative à la protection des données
Des traitements automatisés à grande échelle de données personnelles sensibles ou un profilage à haut risque sont-ils effectués ?	☒	document requis	*Non*	Règlement de traitement

Exemple 2

Y a-t-il un traitement des données personnelles ?	☑	document requis	***Oui***	***Déclaration de confidentialité***
Y a-t-il 250 collaborateurs ou plus ou des données à haut risque sont-elles traitées ?	☑	document requis	***Oui***	***Registre de traitement***
Le traitement de données prévu présente-t-il un risque élevé ?	☑	document requis	***Oui***	***Analyse d'impact relative à la protection des données***
Des traitements automatisés à grande échelle de données personnelles sensibles ou un profilage à haut risque sont-ils effectués ?	☑	document requis	***Oui***	***Règlement de traitement***

Exemple 3

Y a-t-il un traitement des données personnelles ?	☑	document requis	***Oui***	***Déclaration de confidentialité***
Y a-t-il 250 collaborateurs ou plus ou des données à haut risque sont-elles traitées ?	☒	document requis	Non	Registre de traitement
Le traitement de données prévu présente-t-il un risque élevé ?	☒	document requis	Non	Analyse d'impact relative à la protection des données
Des traitements automatisés à grande échelle de données personnelles sensibles ou un	☒	document requis	Non	Règlement de traitement

profilage à haut risque sont-ils effectués ?				
Y a-t-il un transfert du traitement des données personnelles à des tiers ?	☒		Non	Pas de vérification CUU

Exemple 4

Y a-t-il un traitement des données personnelles ?	☑	document requis	***Oui***	***Déclaration de confidentialité***
Y a-t-il 250 collaborateurs ou plus ou des données à haut risque sont-elles traitées ?	☒	document requis	Non	Registre de traitement
Le traitement de données prévu présente-t-il un risque élevé ?	☑	document requis	***Oui***	***Analyse d'impact relative à la protection des données***
Des traitements automatisés à grande échelle de données personnelles sensibles ou un profilage à haut risque sont-ils effectués ?	☒	document requis	Non	Règlement de traitement

Exemple 5

Y a-t-il un traitement des données personnelles ?	☑	document requis	***Oui***	***Déclaration de confidentialité***
Y a-t-il 250 collaborateurs ou plus ou des données à haut risque sont-elles traitées ?	☒	document requis	Non	Registre de traitement
Le traitement de données prévu présente-t-il un risque élevé ?	☒	document requis	Non	*Analyse d'impact relative à la protection des données*
Des traitements automatisés à grande échelle de données personnelles sensibles ou un profilage à haut risque sont-ils effectués ?	☑	document requis	***Oui***	**Règlement de traitement**

Clause de non-responsabilité

Ce guide de mise en œuvre n'est pas une évaluation détaillée des besoins de mise en œuvre des organisations individuelles en ce qui concerne la loi révisée sur la protection des données. Ce guide de mise en œuvre tente plutôt de préparer et de sensibiliser les organisations du secteur à but non lucratif à la nouvelle situation légale. Le guide de mise en œuvre ne répond pas à des questions détaillées et ne prétend pas être exhaustif. En cas de questions spécifiques, il est recommandé de s'adresser à des experts en protection des données.

Glossaire

Sous-traitance	Dans le cadre d'un contrat de sous-traitance, la collecte, le traitement ou l'utilisation de données à caractère personnel, c'est-à-dire le traitement des données, sont confiés à des tiers. Les actions de marketing, les enquêtes auprès des clients et les envois de newsletters par des tiers en sont des exemples.
Obligation de fournir des informations	Toute organisation doit, à la demande d'une personne physique, lui indiquer si des données la concernant sont traitées. Si tel est le cas, l'organisation doit permettre à la personne d'accéder à ses données.
Aspects de la personnalité	Par aspects de la personnalité, on entend, entre autres, des domaines de la personnalité tels que le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, le lieu de résidence ou le déplacement d'une personne physique.
Traitement des données personnelles	Le traitement de données personnelles comprend toute manipulation de données personnelles, par exemple la collecte, l'utilisation, la conservation, la transformation, le traitement, l'exploitation, la communication ou la destruction de données à caractère personnel.
Données personnelles sensibles	Données sur : - l'origine ethnique et la race - opinion politique - Données de santé - données biométriques - données génétiques - les convictions religieuses ou philosophiques - orientation sexuelle
Concept d'effacement	Un concept de suppression est une déclaration ou une description indiquant quand et comment les données à caractère personnel sont supprimées au sein d'une organisation.
Protocole de suppression	Le protocole de suppression permet de consigner de manière générale les jours et les données qui ont été supprimées.
Données personnelles	Les données personnelles sont des données qui se rapportent à une personne physique identifiée ou identifiable. Cette définition théorique peut être très large dans la pratique. Dans certaines circonstances, une

	adresse IP peut déjà être considérée comme une donnée personnelle.
Profilage à haut risque	Dans la loi révisée sur la protection des données, l'expression « profilage à haut risque » désigne toute pratique par laquelle le traitement automatisé de données personnelles prédit ou évalue certains aspects personnels d'une personne physique.
TOM	Mesures techniques et organisationnelles appropriées pour préserver une sécurité des données adaptée au risque. Ces mesures peuvent aller des sauvegardes aux pares-feux en passant par des mots de passe appropriés.
Responsable	Les responsables au sens de la législation sur la protection des données peuvent être des personnes physiques ou morales, mais aussi des autorités ou d'autres organisations et services qui déterminent les finalités et les moyens du traitement des données à caractère personnel.
Délais de prescription	Les délais de prescription découlent des délais de conservation légaux. Ils s'élèvent en général à 10 ans, avec certaines exceptions légales.

Sources et liens utiles

Loi sur la protection des données : https://www.fedlex.admin.ch/eli/cc/2022/491/fr

Ordonnance sur la protection des données (OPDo) sur la protection des données https://www.newsd.admin.ch/newsd/message/attachments/75621.pdf

Dsat, outil d'auto-évaluation de la protection des données :: https://dsat.ch/

ProFonds, Protection des données https://www.profonds.org/fr/defense-des-interets/nouvelle-loi-sur-la-protection-des-donnees-lpd/

FAQ Droit de la protection des données https://www.newsd.admin.ch/newsd/message/attachments/75633.pdf

Commentaire en ligne : Home (onlinekommentar.ch)