

Description de l'Organisation

Nom: Test

Contact: X

Téléphone: +

Email: test.ch

Questionnaire: Analyse d'impact relative à la protection des données

Question: 1 Nom du projet

Réponse: XYZ

Question: 2 Service responsable du projet

Réponse: Z

Question: 3 Quels sont les objectifs de ce projet ?

Réponse: Evaluer les risques qui pèsent sur les données de santé traitées par le XY

Question: 4 Un conseiller à la protection des données indépendant est-il nommé ou prévu pour votre organisation ?

Réponse: Oui

Question: 4.1 Quelle est la fonction de cette personne dans l'entreprise ?

Réponse: Responsable HQSE, hygiène, qualité, santé, environnement

Question: 5 Quelles catégories de données personnelles prévoyez-vous d'utiliser ?

Réponse: Sphère intime et caractéristiques personnelles; Identification de la personne; Identité sens large; Prestations sociales; Famille; Santé

Question: 6 Prévoyez-vous de traiter des données sensibles à savoir des informations relatives à la santé, la sphère intime, les activités ou opinions philosophiques, politiques, syndicales, religieuses, l'aide sociale, les sanctions pénales ou administratives, les poursuites ou origines ethniques ?

Réponse: Oui

Question: 7 Quel est le volume de données personnelles traitées (nb de personnes concernées) ?

Réponse: Plus de 500 personnes

Question: 8 Prévoyez-vous de collecter vous-même les données personnelles ?

Réponse: Oui

Question: 9 S'agit-il de données personnelles que vous obtenez auprès d'un tiers ?

Réponse: Oui

Question: 10 La collecte ou l'exploitation des données se fait-elle sur la base du consentement de la personne, d'une base légale ou réglementaire, d'un intérêt prépondérant ?

Réponse: Consentement de la personne; Intérêt prépondérant; Base légale ou réglementaire

Question: 11 Votre processus de collecte prévoit-il que la personne donne son accord formellement ?

Réponse: Oui

Question: 12 Prévoyez-vous de communiquer les données collectées à l'étranger ? Si oui dans quel pays ?

Réponse: En Europe

Question: 13 Prévoyez-vous de confier certains traitements de données personnelles à des entreprises externes ?

Réponse: Non

Question: 16 Avez-vous élaboré une procédure relative au droit d'accès des personnes concernées ?

Réponse: Oui

Question: 17 Avez-vous prévu que la personne qui fait une demande d'accès prouve son identité ?

Réponse: Oui

Question: 18 Prévoyez-vous de facturer l'accès aux données ?

Réponse: Non

Question: 19 Pouvez-vous garantir que les données que vous traitez sont exactes, intègres et tenues confidentielles ?

Réponse: Oui

Question: 20 Avez-vous déterminé la durée de conservation des données ?

Réponse: Oui

Question: 21 Si nécessaire sera-t-il possible d'effacer les données individuellement ?

Réponse: Je ne sais pas

Question: 22 Si nécessaire sera-t-il possible d'effacer les données en masse ?

Réponse: Oui

Question: 23 Pourrez-vous garantir que la technique choisie permettra de supprimer l'ensemble des données de la personne ?

Réponse: Je ne sais pas

Question: 24 La suppression porte-t-elle aussi sur les sauvegardes ?

Réponse: Je ne sais pas

Question: 25 S'agira-t-il d'un effacement physique ou logique ?

Réponse: Logique; Physique

Question: 26 Quelles mesures techniques ou organisationnelles avez-vous prises pour protéger les données durant leur exploitation ?

Réponse: Classification de l'information; Mesures de défenses (firewall, ...); Journalisation des accès; Gestion des accès

Question: 27 Quelles mesures avez-vous prises pour protéger les données durant leur conservation ?

Réponse: Durée de conservation; Journalisation des accès

Question: 28 Quelles mesures avez-vous prises pour protéger les données durant leur communication ?

Réponse: Journalisation des échanges; Canal sécurisé (VPN)

Question: 29 Envisagez-vous un développement ou une extension du projet dans le futur ?

Réponse: Non

Question: 30 Vous avez fini le questionnaire, avez-vous des remarques générales?

Réponse: non

Faits

Conseiller à la protection des données indépendant est nommé dans l'organisation

Vous avez fait le choix de nommer un conseiller à la protection des données, en interne ou en externe à votre organisation, ce qui est recommandé pour permettre à celle-ci de se mettre en conformité ou de développer ses activités futures de manière conforme aux règles et principes applicables en la matière. Veiller à impliquer cette personne dans la mise en place de tout nouveau projet impliquant le traitement de données personnelles, ce qui permettra à l'organisation de pratiquer la privacy by design and by défaut. Les recommandations découlant de la présente évaluation sont à mettre en œuvre avec son concours.

Données sensibles traitées

Votre projet comprend le traitement de données personnelles sensibles....

Volume des données personnelles traitées

Grand nombre de données personnelles

Données personnelles obtenues auprès d'un tiers

Vous ignorez s'il est prévu de collecter les données personnelles uniquement au sein de l'entreprise ou si la collecte aura également lieu par l'entreprise de tiers, ou vous savez d'ores et déjà que tout ou partie de la collecte se fera par l'entremise de tiers. Dans cette hypothèse, vous devrez garder traces de l'origine des données car cette indication doit être donnée dans le cadre d'une demande de droit d'accès. Si vous n'êtes pas responsable de la manière dont la collecte des données a eu lieu, vous serez cependant tenu à un traitement conforme des données, et devrez veiller par exemple avoir le consentement exprès de la personne concernée s'il s'agit de données personnelles sensibles ou de profil de la personnalité.

Le Processus de collecte prévoit que la personne donne son accord formellement

Le principe de licéité impose que le responsable de traitement dispose d'un motif légitimant celui-ci. Il peut s'agir d'une base légale, du consentement de la personne ou d'un intérêt privé ou public prépondérant. Dans cette dernière hypothèse, c'est au responsable de traitement de motiver l'intérêt rendant le traitement licite. Lorsque le motif légitimant le traitement est le consentement de la personne concernée, il convient de s'assurer que ce consentement soit donné en toute connaissance de cause, et d'une manière expresse lorsqu'il s'agit de données personnelles sensibles ou de profil de la personnalité. Le consentement peut être retiré en tout temps.

Durée de conservation des données

Le principe de proportionnalité (et de minimisation des données pour le Règlement européen) commande que l'on détermine la durée de conservation des données personnelles que l'on traite, ce qui conduit souvent à déterminer la durée de conservation d'un type de document. Les données personnelles ne doivent pas être conservées au-delà de ce qui est nécessaire pour atteindre la finalité pour laquelle elles ont été collectées, ou pour respecter une durée légale de conservation. La loi ne saurait indiquer combien de temps les données personnelles doivent être conservées, le responsable de traitement doit déterminer la durée de conservation qu'il estime nécessaire et qu'il peut justifier. A noter que la durée de conservation peut être longue si la finalité l'exige, mais jamais illimitée. De son côté le droit d'accès garantit à toute personne concernée le droit de faire supprimer les données personnelles dont la conservation n'est plus nécessaire. C'est la raison pour laquelle le responsable de traitement doit pouvoir supprimer une donnée personnelle, quel que soit le support sur lequel elle figure, soit à l'occasion d'une demande individuelle justifiée, soit en raison d'une épuration en masse des données à l'échéance d'un certain délai. La suppression, également appelée effacement, doit être effectuée de manière sûre, irréversible. De manière générale les sauvegardes doivent également être supprimées. Si les sauvegardes sont effectuées de telle manière que les données personnelles ne peuvent plus être traitées d'aucune manière, et donc pas même consultées parce qu'elles ne peuvent plus être reliées à une personne concernée, qu'elles ne peuvent plus permettre l'identification d'une personne, après suppression des données personnelles de base par exemple, on peut considérer que le but est atteint. En revanche, une simple inactivation des données ne correspond pas à une suppression. Dans certains cas, l'anonymisation complète et irréversible peut suffire, voire être préconisée notamment à des fins statistiques. L'archivage à des fins historiques est réservé.

Recommandations priorisées

...