Checklist des exigences de privacy by design pour les développements informatiques

Cette checklist est un extrait traduit de l'anglais par mes soins de la quatrième partie du guide « Software development with Data Protection by Design and by Default » de l'autorité de protection des données norvégienne. L'intégralité du guide peut être consultée sur le site de l'autorité : datatilsynet.no.

1 Explications sur les exigences de protection des données et de sécurité de l'information

Il est nécessaire de savoir au moins

- quelles catégories de données seront traitées ;
- ce qu'on peut déduire de ces données au sujet des individus ;
- qui seront les utilisateurs et quels seront leurs rôles ;
- qui sont les propriétaires/responsables des données ;
- qui est le destinataire des données (à l'interne ou à l'externe).

Seules les données personnelles (absolument) nécessaires au fonctionnement de l'outil, du logiciel, du service, du produit, etc. peuvent être utilisées. Leur cycle de vie doit être pris en considération : une fois devenues inutiles, ou lorsqu'elles ont atteint leur délai de conservation, elles doivent être supprimées. Il est donc nécessaire de connaître au moins :

- le niveau d'information détaillé requis (cf. données nécessaires) ;
- la durée de stockage des données ;
- la possibilité de mettre en place des routines de suppression automatique ;
- le lieu de stockage des données et
- qui aura accès aux données et depuis où.

Des informations claires et concises sur la manière dont les données personnelles seront utilisées sont fondamentales pour garantir la protection des droits des personnes concernées. Celles-ci ont de nombreux droits, dont

- l'accès à toutes leurs données (et l'obtention d'une copie de celles-ci) ;
- l'information au sujet de ce que l'entreprise fait des données ;
- la rectification des données inexactes ;
- la restriction d'utilisation ; et
- la portabilité des données.

L'entreprise doit garantir la sécurité des données, notamment pendant

- leur collecte ;
- leur stockage ;
- leur modification ;
- leur consultation ;

- leur communication et
- leur suppression.

Le chiffrement et le contrôle des accès sont des exemples de mesures qui peuvent être utilisées pour garantir la sécurité. Les exigences de sécurité sont déterminées en identifiant les risques auxquels le produit peut être exposé et les risques que l'entreprise est prête à prendre. Cela permet de définir les paramètres de sélection des mesures pertinentes et correctes pour l'entreprise et le produit.

L'évaluation des risques consiste à identifier les conséquences potentielles de différents incidents ou scénarios, et à évaluer la probabilité ou la facilité avec laquelle un incident indésirable se produit. C'est le management qui détermine le degré de risque que l'entreprise est prête à prendre dans différents scénarios. C'est ce que l'on appelle la tolérance au risque. Ce niveau de tolérance fournit des indications sur les mesures et les ressources à mettre en place pour garantir que le produit ne dépasse pas le niveau de risque acceptable défini.

En termes de sécurité, le niveau de tolérance est défini individuellement pour différents « scénarios de sécurité ». Ces scénarios de sécurité peuvent comprendre, par exemple, l'altération accidentelle de données personnelles, la divulgation non autorisée de données personnelles et un manque d'accessibilité qui pourrait affecter des personnes ou activités.

En termes de protection des données, le niveau de tolérance est défini individuellement pour différents « scénarios de protection des données ». Ces scénarios de protection des données peuvent comprendre la perte de contrôle par la personne concernée sur ses données personnelles, la discrimination de la personne concernée sur la base du profilage effectué par le produit, ou la réidentification d'une personne à partir de données anonymes.

Certains scénarios de sécurité et de protection des données auront une tolérance zéro pour le risque, tandis que pour d'autres, l'entreprise peut être prête à prendre un certain degré de risque. Le management doit fixer des niveaux de tolérance acceptables, c'est-à-dire l'appétit pour le risque, tant pour la protection des données que pour la sécurité.

L'appétit pour le risque de l'entreprise peut être documenté en définissant des niveaux de tolérance pour la protection ou la sécurité des données dans différents scénarios, souvent dans un tableau de référence qui peut être réutilisé pour d'autres évaluations des risques.

Une évaluation des risques commence par la cartographie des valeurs qui doivent être garanties. Le règlement sur la protection des données définit les données personnelles comme une valeur.

Une évaluation de la menace doit être effectuée pour identifier les acteurs qui pourraient être intéressés par les valeurs, et les vecteurs d'attaque utilisés par les différents acteurs de la menace. Une évaluation est ensuite effectuée pour déterminer quelles valeurs sont vulnérables à une menace donnée. Les normes de sécurité de l'information peuvent aider à détecter les vulnérabilités, identifiant ainsi également les exigences qui doivent être établies pour la protection et la sécurité des données.

Le résultat de l'évaluation des risques doit être évalué par rapport au niveau de tolérance de sécurité. Si le niveau de risque est supérieur au niveau prédéterminé de risque acceptable, des mesures doivent être mises en œuvre pour atténuer le risque. Il est également nécessaire de déterminer qui sera responsable de la mesure, et de fixer un délai pour sa mise en œuvre.

L'objectif d'une analyse d'impact sur la protection des données (AIPD) est d'évaluer l'impact qu'un produit ou un traitement envisagé peut avoir sur la protection des données personnelles. Elle vise à garantir que le produit ne porte pas atteinte aux droits fondamentaux de la personne concernée. Pour certains types de traitement de données personnelles, il est nécessaire de procéder à une analyse d'impact sur la protection des données (voir la page Analyse d'impact).

En cas de doute, il est recommandé de procéder à une AIPD. L'évaluation doit contenir au moins :

- une description systématique des traitements envisagés et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
- une évaluation de la nécessité et de la proportionnalité du traitement par rapport aux finalités ;
- une évaluation des risques pour les droits et libertés des personnes concernées ; et
- les mesures envisagées pour faire face aux risques, y compris les garanties, les mesures de sécurité et les mécanismes visant à assurer la protection des données personnelles et à démontrer la conformité avec le règlement relatif à la protection des données en tenant compte des droits et des intérêts légitimes des personnes concernées.

Dans les cas où une AIPD indique que le traitement entraînerait un risque élevé en l'absence de mesures prises pour atténuer le risque, il est impératif de contacter le DPD ou l'autorité de protection des données compétente.

2 Checklist

2.1 Que faut-il faire avant de fixer les exigences ?

☐ Définir le traitement à effectuer, et établir une vue d'ensemble des données personnelles.

- ☐ Les données personnelles seront-elles traitées par le produit ?
- ☐ Identifiez le responsable de traitement, les sous-traitants, etc. Un DPA doit être signé et les sous-traitants doivent être approuvés par le responsable du traitement.
- ☐ Quelle est la base juridique du traitement ?
- ☐ Quelle est la finalité du traitement ?
- ☐ Pendant combien de temps la base juridique et/ou la finalité autorisent-elles le stockage de données personnelles ? Est-il nécessaire de prévoir un effacement automatique ?
- ☐ Définir les catégories de données personnelles qui doivent être traitées pour atteindre la finalité. Le traitement de données sensibles est généralement interdit, à quelques exceptions près. Déterminez si l'une de ces exceptions s'applique. Documentez toute l'étendue des données stockées dans le produit.
- ☐ Comment la transparence est-elle assurée ? Notifications automatiques par le système, tableau de bord de la vie privée, etc.
- ☐ Les données personnelles sont-elles transférées vers un pays tiers ou vers une organisation internationale ? Des conditions s'appliquent au transfert de données personnelles vers des pays tiers ou des organisations internationales, notamment des restrictions en matière d'accès, de fonctionnement et de stockage. Lorsque des données personnelles doivent être transférées vers un pays tiers ou une organisation internationale, il est important de s'assurer que tous ces transferts sont légaux.

☐ Dans quel contexte le traitement aura-t-il lieu ? Est-il probable que le produit puisse être utilisé dans un autre contexte ?

☐ Identifiez toutes les exigences qui s'appliquent à l'entreprise. Existe-t-il des codes de conduite spécifiques à l'industrie ou au secteur ? Existe-t-il des politiques et des exigences qui peuvent vous aider à déterminer les exigences applicables au produit ?

☐ Existe-t-il des systèmes de certification que vous pouvez, et devriez, suivre ? Quelles sont les exigences applicables dans ce cas ?

☐ L'autorité (suisse ou européenne) chargée de la protection des données a-t-elle pris des décisions dans ce domaine, concernant l'entreprise ou d'autres entreprises comparables, qui devraient être incluses dans les exigences du produit ?

2.2 Exigences en matière de protection des données et de sécurité

☐ Si le produit fonctionne comme prévu sans données personnelles, aucune donnée personnelle ne doit être collectée.

☐ La protection des données peut être conçue en utilisant des techniques de pseudonymisation dans le produit.

☐ Une identification inutile et des données personnelles redondantes dans le produit entraînent un risque accru pour l'utilisateur ou la personne concernée. Cela rend également le produit plus vulnérable et plus attrayant pour les acteurs qui souhaitent réutiliser les données à d'autres fins.

☐ Le produit doit utiliser les données personnelles comme prévu, et toutes les données doivent être supprimées lorsque leur conservation n'est plus légale ou n'est plus nécessaire pour atteindre l'objectif.

☐ Les données personnelles doivent être accessibles aux personnes autorisées lorsque c'est nécessaire.

☐ Le produit doit être développé avec des paramètres par défaut qui protègent les droits des personnes concernées et préservent la vie privée.

☐ Le produit doit guider l'utilisateur vers le mode d'utilisation le plus respectueux de la vie privée.

2.3 Exigences relatives aux principes de protection des données

Les exigences de base pour les produits utilisés pour traiter les données personnelles sont les suivantes :

☐ Le traitement des données personnelles dans le produit n'est licite que si l'une des conditions suivantes est remplie :

☐ la personne concernée a donné son consentement ;

☐ le traitement est nécessaire à l'exécution d'un accord ou d'un contrat écrit avec la personne concernée ;

☐ le traitement est nécessaire au respect d'une obligation légale ;

☐ le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

☐ le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique ;

☐ le traitement est nécessaire à la réalisation des finalités d'intérêts légitimes poursuivies par le responsable du traitement (mise en balance des intérêts).

☐ Le produit doit garantir des paramètres par défaut qui protègent les droits des personnes concernées et préservent la vie privée.

☐ Le traitement des données personnelles doit être prévisible par la personne concernée et effectué dans le respect des intérêts de cette dernière.

☐ Le produit doit être conçu afin que les aspects pertinents du traitement des données personnelles soient connus de la personne concernée, afin que celle-ci puisse prendre des décisions en connaissance de cause ou exercer ses droits.

☐ Le produit doit veiller à ce que d'autres droits, tels que l'absence de discrimination, soient sauvegardés.

☐ Des informations claires et compréhensibles doivent être fournies à la personne concernée concernant la finalité du traitement des données personnelles, la base juridique, les destinataires des informations.

☐ Le produit ne doit collecter des données personnelles qu'à des fins précises, explicites et légitimes.

☐ Les données personnelles ne doivent pas être traitées ultérieurement d'une manière incompatible avec les finalités initiales.

☐ Le produit ne doit traiter que les données personnelles qui sont adéquates, pertinentes et limitées à ce qui est nécessaire par rapport aux objectifs pour lesquels elles sont traitées.

☐ Le produit doit garantir que toutes les données personnelles sont exactes et à jour. Les données incorrectes doivent être supprimées ou rectifiées.

☐ Le produit doit garantir qu'il n'est pas possible d'identifier la personne concernée plus longtemps que ce qui est strictement nécessaire aux fins pour lesquelles les données personnelles sont traitées.

☐ Le produit doit assurer une sécurité appropriée des données personnelles.

Si le produit nécessite un consentement :

☐ Le consentement doit être explicite (pas passif), volontaire (pas de contrainte/pression) et informé (prévisible).

☐ Le traitement fondé sur le consentement doit être clairement distingué des autres éléments.

☐ Une déclaration de consentement doit être rédigée dans un langage clair et simple, et être intelligible et facilement accessible au lecteur. Des conditions distinctes s'appliquent aux enfants.

☐ Les utilisateurs doivent pouvoir retirer leur consentement à tout moment et aussi facilement qu'ils le donnent.

2.4 Exigences relatives aux droits des personnes concernées

L'obligation d'information diffère selon que les données personnelles sont obtenues auprès de la personne concernée ou qu'elles sont obtenues directement à partir d'un système ou de personnes autres que la personne concernée.

Lorsque des données personnelles sont obtenues de la personne concernée, celle-ci doit savoir :

☐ qui est le responsable du traitement des données (identité et coordonnées) ;

- ☐ qui est le DPD ;
- ☐ la raison pour laquelle leurs données personnelles sont traitées (à quelle fin) ;
- ☐ quelle est la base juridique du traitement (consentement, contrat, etc.) ;
- ☐ quels sont les intérêts légitimes, le cas échéant ;
- ☐ à qui les données seront communiquées (destinataires), y compris les sous-traitants et unités à l'interne ;
- ☐ si les données sont transférées à un pays tiers ou à une organisation internationale ;
- ☐ quelle est la durée de conservation des données ;
- ☐ comment elle peut exercer ses droits (d'accéder à ses données personnelles, de les rectifier et de les effacer, de s'opposer au traitement, d'y apporter des restrictions, d'en demander la portabilité) ;
- ☐ que son consentement peut être retiré à tout moment ;
- ☐ si le traitement des données personnelles est effectué en raison d'exigences contractuelles ou s'il est nécessaire pour la conclusion d'un contrat ;
- ☐ si l'utilisation du produit implique une prise de décision automatisée ou un profilage, auquel cas il convient également de lui fournir des informations sur les algorithmes et la signification/les conséquences du traitement ;
- ☐ si les données personnelles sont destinées à être utilisées à des fins autres que celles pour lesquelles elles ont été collectées et, dans l'affirmative, quels droits et réglementations s'appliquent à ce traitement.

Lorsque des données personnelles sont collectées auprès de personnes autres que la personne concernée, des informations doivent être fournies concernant

- ☐ les catégories de données personnelles traitées ;
- ☐ la ou les sources des données personnelles et si elles proviennent de sources accessibles au public.

Le produit doit permettre à la personne concernée d'exercer facilement ses droits, tels que

- ☐ le droit d'accéder à leurs données personnelles, aux informations sur le traitement et à d'autres droits ;
- ☐ le droit de rectifier leurs données personnelles le plus rapidement possible ;
- ☐ le droit d'effacer leurs données personnelles le plus rapidement possible, si les conditions d'effacement sont remplies (droit à l'oubli) ;
- ☐ le droit à la limitation du traitement de leurs données personnelles, si les conditions de limitation sont remplies ;

- ☐ le droit à la portabilité des données personnelles les concernant, si le traitement est fondé sur un consentement ou un contrat et s'il est effectué par des moyens automatisés ;
- ☐ le droit de s'opposer au traitement de leurs données personnelles, si les conditions d'opposition sont réunies ;
- ☐ les droits relatifs à la prise de décision individuelle automatisée, y compris le profilage, qui peut avoir des conséquences juridiques, ou un effet tout aussi important pour la personne concernée.

Si l'utilisateur a demandé que les données personnelles soient rectifiées, supprimées ou limitées, le responsable du traitement doit en informer chaque destinataire auquel les données personnelles ont été communiquées.

Le produit doit pseudonymiser les données personnelles lorsqu'il n'est plus nécessaire de disposer de données personnelles et anonymiser ou supprimer les données personnelles lorsque la finalité du traitement est atteinte.

Le produit doit contenir des garanties empêchant la mise en relation de données personnelles d'une personne avec d'autres données personnelles dans d'autres systèmes, ou avec des données personnelles collectées à d'autres fins.

2.5 Exigences relatives à la sous-traitance

L'entreprise ne doit faire appel qu'à des sous-traitants qui offrent des garanties suffisantes, qui mettront en œuvre des mesures assurant la protection des droits des personnes concernées et sauvegardant les intérêts de l'entreprise. L'entreprise doit s'assurer que tous les fournisseurs et sous-traitants remplissent toutes les exigences en concluant des DPA.

2.6 Exigences relatives à la sécurité des traitements

Pour garantir la sécurité du traitement des données personnelles, il est nécessaire de

- ☐ garantir la confidentialité (C). Les données personnelles doivent être protégées contre toute divulgation ou tout accès non autorisé ;
- ☐ assurer l'intégrité (I). Les données personnelles doivent être protégées contre la destruction, la perte ou l'altération accidentelle et illégale ;
- ☐ assurer l'accessibilité (A). Les données personnelles doivent être accessibles au personnel autorisé qui en a besoin pour son travail ;
- ☐ garantir la résilience (R). La résilience signifie que les produits qui traitent des données personnelles doivent être capables de résister, par exemple, aux vulnérabilités, aux attaques et aux accidents ;
- ☐ assurer la traçabilité (T). La traçabilité est la documentation des modifications apportées au sein du produit et aux données personnelles. L'objectif de la traçabilité est de gérer les failles de sécurité.

Ci-dessous, les exigences CIART plus en détail.

- ☐ Contrôle d'accès

☐ Le produit dispose d'un contrôle d'accès (autorisation, authentification et traçabilité).

- ☐ Les utilisateurs doivent être identifiés. (T)
- ☐ Il décide des rôles et des droits associés (principe du moindre privilège). (A)
- ☐ Il est possible de contrôler la traçabilité lors de l'audit des journaux. (T)

☐ Les utilisateurs n'ont accès qu'aux informations nécessaires à l'accomplissement de leurs tâches individuelles (principe du moindre privilège). (C, T)

☐ Les privilèges d'administrateur sont accordés à un petit nombre de personnes sur la base du principe du moindre privilège. (C, I, A, R, T)

☐ Les personnes concernées ont accès à leurs données personnelles. (I, A)

☐ Les mots de passe sont gérés de manière sécurisée et le produit nécessite des mots de passe forts. (C, I, A)

☐ Le produit prend en charge et exige une authentification forte (telle que l'authentification à deux facteurs) lorsque cela est nécessaire (par exemple, les utilisateurs peuvent être encouragés à l'utiliser, tandis qu'il est exigé des administrateurs et des utilisateurs ayant accès à des données personnelles nécessitant une protection ou à des données personnelles sur plusieurs sujets). (C, I, T)

☐ Le produit doit surveiller si et quand quelqu'un tente d'obtenir un accès non autorisé. (C, I, R, T)

☐ Le produit doit restreindre l'accès des tiers et limiter ce à quoi un tiers peut accéder (par exemple, restreindre l'accès à des adresses IP spécifiques ou fournir un accès temporaire et limité). (C, I, R)

☐ Le produit doit garantir une sécurité de l'information appropriée et suffisante lors du stockage et de la communication des données. Le chiffrement peut aider à atteindre cet objectif. Lors de l'utilisation du chiffrement, des algorithmes et des méthodes répandus et reconnus doivent être utilisés à tout moment, avec une longueur de clé suffisante. Des exigences minimales doivent être fixées pour l'administration, en précisant à quelle fréquence les algorithmes de sécurité doivent être examinés et mis à jour :

- ☐ aux points d'extrémité (PC, ordinateur portable, téléphone, tablette) ; (C, R)
- ☐ lors de l'accès à distance ; (C, R)
- ☐ lors du transfert et du stockage via les services en nuage ; (C, R)
- ☐ pour les copies de sauvegarde et de sécurité, et les unités contenant des données de sauvegarde. (C, A, R)

☐ Le produit doit protéger l'intégrité des données et être capable de détecter les changements dans les fichiers, les serveurs et les réseaux, en (I)

- ☐ comparant les valeurs de hachage et les sommes de contrôle ;
- ☐ limitant l'accès en écriture par
  - ☐ des contrôles d'intégrité réguliers ;
  - ☐ la fixation de valeurs de référence (min/max).

☐ Le produit doit garantir que les données personnelles sont disponibles en cas de besoin par le biais de (A)

- ☐ la redondance ;
- ☐ plans d'urgence ;
- ☐ la gestion des incidents.
- ☐ Le produit doit être capable de rétablir la disponibilité et l'accès aux données personnelles en temps utile en cas d'incident physique ou technique.

☐ Le produit doit être résilient. Il doit (R)

- ☐ être protégé contre les failles de sécurité et les vulnérabilités connues ;
- ☐ être correctement configuré ;
- ☐ assurer la segmentation des données stockées, des systèmes, des processeurs et des réseaux ;
- ☐ veiller à ce que les produits et les correctifs de tiers soient tenus à jour ;
- ☐ être capable de recevoir des notifications des utilisateurs et d'autres personnes concernant les vulnérabilités du produit, et de veiller à ce qu'elles soient gérées et prises au sérieux ;
- ☐ assurer la destruction sécurisée des supports qui traitent des données personnelles.

☐ Le produit doit permettre de retracer les modifications et de gérer les failles de sécurité par (T)

- ☐ la documentation des produits et des procédures ;
- ☐ l'enregistrement des changements de configuration, des processus, des activités et des incidents ;
- ☐ le contrôle de l'accès aux journaux sur la base du principe du moindre privilège et uniquement lorsque l'accès est spécifiquement requis ;
- ☐ Il faut supprimer ou anonymiser les journaux après une date limite donnée et ne pas les conserver plus longtemps que nécessaire.

2.7 Exigences relatives à la définition du niveau de risque acceptable pour l'entreprise

☐ Établir des niveaux de tolérance pour la protection des données et la sécurité de l'information. L'objectif de la fixation de niveaux de tolérance est de définir des niveaux de risque acceptables pour la sécurité et la protection des données dans le produit. Ces niveaux doivent être basés sur des limites de tolérance établies et acceptées.

☐ Définir des niveaux individuels acceptables de risque pour la protection des données et la sécurité de l'information.

Exemples de catégories qui doivent présenter des niveaux de risque acceptables pour la protection des données :

☐ La personne concernée doit avoir le contrôle de ses données personnelles.

☐ La personne concernée ne doit pas perdre ses droits ou ses libertés.

☐ La personne concernée ne doit pas faire l'objet de profilage ou de discrimination.

☐ La personne concernée ne doit pas faire l'objet d'une usurpation d'identité ou d'une fraude.

☐ La personne concernée ne doit pas subir de pertes financières.

☐ La personne concernée ne doit pas subir de perte de réputation.

☐ En cas de pseudonymisation, il ne doit pas être possible de retrouver l'identité d'origine sans autorisation.

☐ La confidentialité des données protégées ne doit pas être violée.

Exemples de catégories qui doivent présenter un niveau de risque acceptable pour la sécurité :

☐ Il ne doit pas y avoir de destruction, de perte ou d'altération accidentelle ou illicite de données personnelles.

☐ Il ne doit pas y avoir de divulgation ou d'accès non autorisé à des données personnelles.

☐ Les données personnelles doivent être sécurisées en ce qui concerne la confidentialité, l'intégrité, l'accessibilité et la résilience du logiciel.

☐ Les données personnelles doivent être pseudonymisées aussi rapidement que possible et chiffrées.

☐ La disponibilité et l'accès aux données personnelles doivent pouvoir être rétablis en temps utile en cas d'incident physique ou mental.

☐ Il doit exister un processus permettant de tester, d'apprécier et d'évaluer régulièrement l'efficacité des mesures visant à garantir la sécurité du traitement.

