COFACE

Annexe 06

Protection des données dès la Conception, Protection des données par défaut et Analyse d'Impact sur la Protection des Données

Protection des données dès la Conception, Protection des données par défaut et Analyse d'Impact sur la Protection des Données

Table des matières

1. Objectifs et Champ d'Application

1.1 Objectifs

Protection des données dès la Conception

La Protection des données dès la Conception est une approche qui vise à assurer la protection de la vie privée des individus. Elle se caractérise par la prise en compte de considérations de protection de la vie privée dès le début du développement des produits, des services, des pratiques commerciales et des infrastructures physiques.

Protection des données par défaut

Le principe de Protection des données par défaut vise à mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir que, par défaut :

- seules les données personnelles nécessaires à chaque finalité spécifique du traitement sont traitées ;
- la période de conservation est limitée pour répondre à la finalité spécifique ;
- l'accès aux données personnelles est limité pour répondre à la finalité spécifique ;
- les données personnelles sont traitées avec la plus haute protection de la vie privée disponible ;
- tous les paramètres pertinents pour la protection des données, qui peuvent ensuite être modifiés par la personne concernée elle-même, sont initialement désactivés ou réglés sur "aucun / moins de traitement des données" lorsqu'ils sont mis en service.

Ce principe se réfère aux choix faits par les entités Coface concernant toute valeur de configuration préexistante ou option de traitement assignée dans une application logicielle, un programme informatique ou un appareil.

Analyse d'Impact sur la Protection des Données

L'analyse d'impact sur la protection des données est régie par l'article 35 du RGPD et basée sur les principes et vérifications élaborés par le groupe de travail Article 29 sur la protection des données (G29) dans leur directive WP 248 du 4 avril 2017. L'AIPD sera utilisée pour évaluer l'impact sur la vie privée d'un projet, et peut concerner une ou plusieurs opérations de traitement des données.

Respect des principes de Protection des données dès la Conception, par Défaut et Analyse d'Impact sur la protection des données

Coface reconnaît les principes de Protection des données dès la Conception, par défaut et d'évaluation d'impact sur la protection des données, cela afin de :

- se conformer à la loi, ces principes et instruments étant imposés par les articles 25 et 35 du RGPD;
- respecter les droits et libertés des personnes physiques en ce qui concerne leurs données personnelles ;
- réduire les coûts, car il est empiriquement prouvé que les traitements de données ayant intégré les procédures de Protection des données dès la Conception, par défaut et les procédures d'évaluation d'impact sur la protection des données, entraînent des coûts de fonctionnement significativement inférieurs aux traitements réalisés sans ces procédures.

Risques

Coface est consciente des risques qui peuvent survenir sans l'application de la Protection des données dès la Conception, par défaut et, si nécessaire, de l'évaluation d'impact sur la protection des données, et en particulier :

- Incapacité à démontrer la conformité et la résilience d'une organisation de protection des données aux autorités et aux personnes concernées (comme l'exige l'article 24 du RGPD) ;
- Mauvaise gestion des droits des personnes concernées avec des plaintes subséquentes, impliquant les autorités ;
- Augmentation du nombre de violations de données personnelles ;
- Dégradation de l'image de marque ;
- Coûts significativement accrus pour les mises en œuvre rétroactives de fonctionnalités.

1.2 Champ d'Application

Cette procédure s'applique à tous les chefs de projet Coface, responsables d'applications, de produits, de processus et sponsors de projets qui sont responsables de la planification ou de la modification de nouvelles applications, processus ou produits pour le traitement des données personnelles.

2. Procédure

Le cadre de la Protection des données dès la Conception, par défaut et de l'Analyse d'Impact sur la Protection des Données (AIPD) se compose de deux phases clés.

2.1. L'évaluation des risques de la Protection des données dès la Conception et par défaut

(1) L'évaluation des risques de la protection des données

- Le chef de projet ou le responsable de l'application doit réaliser une liste de contrôle de "Evaluation des risques de la protection des données" (telle que disponible actuellement) qui attribue des points de risque en fonction des catégories de données prévues pour le traitement, de la présence d'indicateurs de risque élevé et de la présence d'environnements techniques particuliers pouvant entraîner des risques plus élevés.

(2) La vérification des résultats par le Délégué à la Protection des Données du Groupe et l'application de la Protection des données dès la Conception et par défaut

- Le Délégué à la Protection des Données du Groupe vérifie la compréhension et la cohérence des résultats, en tenant compte du projet spécifique. Si nécessaire, le score est ajusté en consultation avec le chef de projet.
- En fonction du score final, le Délégué à la Protection des Données du Groupe déterminera si une AIPD doit être réalisée, deux conditions devant être remplies :

- Le score final est de 10 ou plus, et
- Au moins un des indicateurs de risque élevé doit être positif.

- Si deux indicateurs de risque élevé sont positifs (ce qui conduit à un score final de 10 ou plus), une analyse d'impact sur la protection des données est obligatoire.
- S'il n'est pas nécessaire de réaliser une AIPD, le Délégué à la Protection des Données doit ajouter une note de recommandation obligatoire sur la Protection des données dès la Conception et par défaut aux documents du projet. Cette recommandation doit aborder tous les éléments ou des éléments spécifiques du "Répertoire de la Protection des données dès la Conception et par Défaut" (tel que disponible actuellement) et indiquer quels modèles de Protection des données dès la Conception et par défaut doivent être pris en compte en fonction de la nature du projet.

2.2 Analyse d'Impact sur la Protection des Données

Vérifications obligatoires

Si un projet doit faire l'objet d'une analyse d'impact sur la protection des données, celle-ci doit inclure les vérifications listées dans l'annexe 1.

Parties prenantes

L'analyse d'impact sur la protection des données doit être réalisée par toutes les parties prenantes impliquées dans le projet :

- **Le chef de projet**, responsable de la mise en œuvre du projet, reste le premier point de contact concernant toutes les exigences techniques, énoncées par la Protection des données dès la Conception et la Protection des données par défaut.
- **Le sponsor** examinera, en tant que premier niveau de défense, l'analyse d'impact sur la protection des données. Il présentera également l'avancement du projet au conseil d'administration.
- **Le Délégué à la Protection des Données du Groupe (GDPO)** a la charge d'identifier les risques élevés en matière de protection des données au sein du pays / de l'entité, et de confirmer au sponsor et au chef de projet si une consultation obligatoire préalable doit être réalisée auprès de l'autorité de contrôle.
- **Le Responsable de la Sécurité des Systèmes d'Information (CISO)** fournira son expertise sur les sujets de sécurité informatique et sur sa connaissance de l'architecture informatique du Groupe.
- **Les départements Juridiques et Conformité** ont pour principale responsabilité de soutenir et conseiller le chef de projet sur des sujets spécifiques pour lesquels leur expertise est requise.

Application de la Protection des données dès la Conception et par défaut

Dans tous les aspects techniques du projet et dans le cadre des examens obligatoires de l'Annexe 1 ci-dessous, le document « Répertoire de la Protection des données dès la Conception et par Défaut » doit à nouveau être considéré comme une source primaire obligatoire.

En fonction des risques que le projet présente pour les personnes concernées, le Délégué à la Protection des Données du Groupe déterminera si le contenu du Répertoire de la Protection des données dès la Conception et par défaut offre une protection suffisante, ou si d'autres mesures de protection ou d'amélioration de la confidentialité doivent être envisagées.

Documentation

Toutes les vérifications obligatoires de l'annexe 1, leurs résultats et considérations, y compris l'avis final du Délégué à la Protection des Données du Groupe, doivent être documentés dans :

- la documentation du projet ;
- le registre des activités de traitement, tenu par le Délégué à la Protection des Données du Groupe.

3. Annexe I – Vérifications Obligatoires de l'Analyse d'Impact sur la Protection des Données

Analyse d'Impact sur la Protection des Données – Vérifications Obligatoires (Articles du RGPD)

- ☐ une description systématique des opérations de traitement est fournie (Article 35(7)(a)):
  - ☐ la nature, la portée, le contexte et des finalités du traitement sont prises en considération (considérant 90) ;
  - ☐ les données personnelles, le destinataires et la période de conservation des données personnelles sont enregistrées ;
  - ☐ une description fonctionnelle de l'opération de traitement est fournie ; les actifs sur lesquels reposent les données personnels (matériel, logiciel, réseaux, personnes, papier ou canaux de transmission papier) sont identifiées ;
  - ☐ le respect de codes de conduit approuvés est prise en considération (Article 35(8));
- ☐ la nécessité et la proportionnalité sont évaluées Article 35(7)(b)):
  - ☐ les mesures envisages pour se conformer au règlement sont déterminées (Article 35(7)(d) et considérant 90), cela en tenant compte :
    - ☐ des mesures contribuant à la proportionnalité et à la nécessité du traitement sur la base de :
      - ☐ ses finalités déterminées, explicites et légitimes (Article 5(1)(b));
      - ☐ la licéité du traitement (Article 6);
      - ☐ l'adéquation, la pertinence et la limitation des données personnelles à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (Article 5(1)(c));
      - ☐ la limitation dans le temps de la durée de conservation (Article 5(1)(e));
    - ☐ des mesures contribuant aux droits des personnes concernées:
      - ☐ information fournie à la personne concernée (Articles 12, 13 et 14);
      - ☐ droit d'accès et droit à la portabilité des données (Articles 15 et 20);
      - ☐ droit de rectification et droit à l'effacement (Articles 16, 17 et 19);
      - ☐ droit d'opposition et droit à la limitation du traitement (Articles 18, 19 et 21);
      - ☐ relations avec les sous-traitants (Article 28);
      - ☐ les garanties entourant les transferts de données vers des pays tiers ou à des organisations internationales (Chapitre V);
      - ☐ la consultation préalable (Article 36).
  - ☐ les risques pour les droits et libertés des personnes concernées sont évalués (Article 35(7)(c)):
    - ☐ l'origine, la nature, la particularité et la gravité des risques sont appréciés (considérant 84) ou, plus spécifiquement, pour chaque risque (accès illégitime, modification indésirable et disparition des données) du point de vue des personnes concernées :
      - ☐ les sources de risques sont prises en compte (considérant 90) ;
      - ☐ les impacts potentiels sur les droits et libertés des personnes concernées sont identifiés en cas d'événements incluant l'accès illégitime, la modification indésirable ou la disparition des données ;
      - ☐ les menaces pouvant conduire à l'accès illégitime, à la modification indésirable et à la disparition des données sont identifiées ;

- ☐ la probabilité et la gravité sont estimées (considérant 90);
- ☐ les mesures envisagées pour traiter ces risques sont déterminées (Article 35(7)(d) et considérant 90);

☐ <u>Les parties intéressées sont impliquées :</u>

- ☐ L'avis du Délégué à la Protection des Données du Groupe est sollicité (Article 35(2));
- ☐ Les avis des personnes concernées ou de leurs représentants sont sollicités, le cas échéant (Article 35(9)).