Contrôles-clés de l'organisation de la protection des données

Groupe de travail Audit interne & protection des données de l'IIA Allemagne (DIIR)

Traduit et adapté par

ifaci
institut français de l'audit et du contrôle internes

DIIR
Deutsches Institut für Interne Revision e.V.

Préface

Le Règlement général de l'Union Européenne sur la Protection des Données (RGPD), les législations nationales correspondantes (en particulier la loi fédérale allemande révisée et les textes de transposition en France) ainsi que, le cas échéant, les instructions des autorités régionales et locales (cas des Länder en Allemagne) donnent un élan particulier à la protection des données. Il en résulte des exigences plus strictes pour l'instauration d'une organisation documentée et efficace de la protection des données, en particulier en ce qui concerne les responsabilités et les risques de sanction (amende administrative pouvant aller jusqu'à 20 millions d'euros ou jusqu'à 4% du chiffre d'affaires annuel du groupe).

Le groupe de travail Audit interne & Protection des données de l'IIA Allemagne (DIIR) propose ci-après une procédure (sous forme d'une check-list) de vérification de l'organisation de la protection des données et de son efficacité dans l'entreprise. Cette liste de contrôles-clés a été conçue à la fois pour une vérification de l'état de préparation à la mise en conformité au RGPD (jusqu'à mai 2018) et pour des missions d'audit de suivi. Indépendamment des missions, cet aperçu peut représenter un cadre important pour les approches et réglementations à respecter dans le contexte de la protection des données.

Cette check-list a été établie selon l'état actuel de la réglementation et des connaissances. Elle ne prétend être ni obligatoire ni exhaustive et ne se substitue en aucun cas à la vérification de la situation juridique de chaque entreprise.

1 Stratégie de protection des données

Une stratégie désigne un concept général ou une orientation pour la réalisation à long terme des buts et objectifs spécifiques de l'entreprise. Une stratégie ne donne qu'une direction générale du développement de l'entreprise. C'est pourquoi elle doit être concrétisée par des décisions ultérieures. Parallèlement, une stratégie nécessite un ajustement permanent à des conditions qui ne cessent d'évoluer. De même, la stratégie de protection des données constitue l'élément central pour l'application des exigences légales et des règles existantes concernant le traitement des données à caractère personnel dans l'entreprise.

1.1 Eléments fondamentaux

L'article 25 du RGPD (considérant 78) incite le responsable du traitement à disposer d'une stratégie appropriée de traitement des données. C'est cette stratégie qui orientera les contrôles du délégué à la protection des données prévus à l'article 39.1.b du RGPD.

- Existe-t-il une stratégie de protection des données et comment est-elle formalisée ?
- La stratégie est-elle applicable à l'ensemble de l'entreprise/du groupe ?
- Quand la stratégie a-t-elle été adoptée/actualisée ?
- Avec qui la stratégie a-t-elle été convenue ? Les organismes internes/externes requis ont-ils été impliqués ?
- Qui a adopté la stratégie ?
- Quelles sources (droit national, référentiels, bonnes pratiques, etc.) ont été utilisées pour élaborer la stratégie ?
- Quels sont les éléments fondamentaux et les principes de la stratégie ?
- La stratégie est-elle appropriée/plausible, en particulier au regard de la taille, de la structure de l'entreprise, de son modèle économique, de ses implantations géographiques et de la nature des données ?
- La stratégie tient-elle suffisamment compte des exigences légales en vigueur (p. ex. article 25 du RGPD) ?
- La stratégie est-elle cohérente avec le modèle de gouvernance de l'entreprise ?

- Toutes les sociétés /entités légales du groupe ont-elles l'obligation d'appliquer la stratégie ?
- Qui suit la mise en œuvre de la stratégie ?
- Existe-t-il des règles d'entreprise contraignantes relatives à la protection des données approuvées par les autorités de contrôle compétentes au sens du RGPD (article 47) (p.ex. Binding Corporate Rules ou règles d'entreprise contraignantes lors de transferts de données de l'entreprise ou du groupe vers des pays tiers) ?

1.2 Mise en œuvre et communication

La stratégie doit être constituée de principes applicables dans l'ensemble de l'entreprise par la mise en œuvre de procédures et d'actions concrètes. Conformément à l'article 5.2 du RGPD, le responsable du traitement doit pouvoir démontrer le respect de ces exigences.

- Comment la stratégie a-t-elle été diffusée ?
- Comment la stratégie et les exigences ont-elles été communiquées dans toute l'entreprise et les groupes cibles formés/sensibilisés (conception et planification de la communication) ?
- Existe-t-il une approche en matière de surveillance et de reporting ?
- Existe-t-il au sein de l'entreprise un référentiel de contrôle interne formalisé intégrant les questions de protection des données ?
- Dans le cadre du référentiel de contrôle interne, les processus/contrôles/objectifs de contrôle et responsabilités concernant la protection des données sont-ils documentés ?
- Dans le cadre de la gestion de la sécurité (informatique et physique - surveillance des bâtiments, etc.) les processus/contrôles/objectifs de contrôle et responsabilités adéquats concernant la protection des données sont-ils documentés ?

2 Règles et exigences

Les principes à respecter résultent des lois nationales/internationales applicables à l'intérieur et à l'extérieur de l'Union Européenne, des règles sectorielles, des exigences internes à l'entreprise et de la jurisprudence. En particulier, la connaissance de ces dispositions et leur mise en œuvre dans les processus internes sont déterminantes pour l'audit. En l'absence de principes contraignants, opérationnels et robustes dans la stratégie de protection des données, des règles internes devront accompagner leur mise en œuvre effective.

2.1 Règles en matière de protection des données, exigences légales et internes

- Existe-t-il des règles d'entreprise contraignantes émises par la direction ?
- Les règles d'entreprise contraignantes tiennent-elles compte des lois, des normes et référentiels correspondant au cadre légal et spécifiques au secteur ?
- Existe-t-il d'autres exigences légales et/ou internes ? Dans l'affirmative, sont-elles cohérentes entre elles ?
- Existe-t-il des conventions collectives ou d'entreprise ?
- Est-il tenu compte du fait que le RGPD s'applique aussi à toutes les entreprises établies hors de l'Union Européenne, pour autant qu'elles proposent des biens ou des services à des personnes concernées au sein de l'UE ou qu'elles observent le comportement de ces personnes (champ d'application territorial des activités quelle que soit la localisation du traitement, cf. article 3 du RGPD) ?
- Les exigences sont-elles cohérentes entre elles et a-t-on l'assurance que les exigences obligatoires ou les plus strictes correspondent aux dispositions réglementaires ?

2.2 Respect des exigences locales

Le RGPD contient des clauses de flexibilité pour le législateur national ainsi que des mandats législatifs concrets adressés aux Etats membres. Certaines dispositions nécessitent une adaptation du droit national en matière de protection des données. En Allemagne, la loi fédérale révisée[1] sur la protection des données (BDSG-neu) complète le RGPD directement applicable. En outre, des adaptations similaires sont à prévoir dans les lois régionales sur la protection des données.

- L'entreprise tombe-t-elle dans le champ d'application de la loi fédérale allemande relative à l'adaptation et à la mise en œuvre de la protection des données (DSAnpUG-EU)[2] ?
- Existe-t-il d'autres dispositions légales de la Fédération sur la protection des données qui priment sur les dispositions de la DSAnpUG-EU / loi révisée sur la protection des données ?
- Leurs contenus réglementaires essentiels sont-ils observés ?
  - Licéité du traitement (article 47 de la loi fédérale allemande relative à la protection des données, article 6 du RGPD)
  - Consentement (article 51 de la loi fédérale allemande relative à la protection des données, article 7 du RGPD)
  - Catégories particulières de données à caractère personnel (article 51(5) de la loi fédérale allemande relative à la protection des données, article 9 du RGPD)
  - Devoirs d'information et droits d'accès (articles 32,33, 34 de la loi fédérale allemande relative à la protection des données, articles 12, 14, 15, 18 du RGPD)
  - Surveillance vidéo (article 4 de la loi fédérale allemande relative à la protection des données)

Le RGPD nécessite des adaptations dans certains domaines. Principalement :

- L'autorisation de collecte et de traitement des données à caractère personnel
  - Pour l'essentiel, pas de changement par rapport à l'ancienne loi fédérale allemande sur la protection des données.

---

[1] La loi fédérale allemande révisée relative à la protection des données dite « BDSG-neu » (neue Bundesdatenschutzgesetz) du 30 juin 2017 modifie la loi initiale de 1977 (Bundesdatenschutzgesetz) dans le cadre de l'adoption du RGPD. Elle est entrée en vigueur le 25 mai 2018.
NdT : En France, la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles modifie la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dans le cadre de l'adoption du RGPD.
https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte

[2] La loi dite « DSAnpUG-EU » (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU) est la loi d'adaptation et de mise en œuvre du RGPD en Allemagne. Elle reprend la BDSG-neu dans son premier article et modifie d'autres lois allemandes existantes.

    - Même dans le cas du RGPD, une interdiction avec réserve d'autorisation (cf. article 6 du RGPD) s'applique :
        - Obligation légale
        - Contrat / Mesures précontractuelles (acte juridique)
        - Intérêt prépondérant
        - Compatibilité avec les finalités initiales
        - Consentement
        - Sauvegarde des intérêts vitaux
- L'adaptation de l'organisation de la protection des données
    - Politiques de protection des données et de sécurité du traitement
    - Technologies respectueuses de la vie privée (article 25 du RGPD)
    - Sécurité du traitement selon l'état des connaissances, le contexte et les risques (article 32 du RGPD)
    - Obligations de documentation du respect des principes relatifs au traitement des données à caractère personnel (article 5 du RGPD)
        - Gestion de la protection des données
        - Responsabilités
        - Registre des activités de traitement (article 30 du RGPD)
        - Analyse d'impact relative à la protection des données, y compris l'évaluation des risques (article 35 du RGPD)
        - Contrôle du respect du RGPD et d'autres exigences en matière de protection des données ainsi que des stratégies de protection des données du responsable du traitement ou du sous-traitant (article 39 RGPD)
    - Mise en œuvre des droits des personnes concernées y compris le devoir d'information
- Le devoir d'information (article 13 f. du RGPD) lors de la collecte directe ou indirecte de données à caractère personnel.
- L'adaptation des sites internet et des déclarations de confidentialité (article 13 f. du RGPD).
- Le transfert de données vers des pays tiers
    - Constatation de l'adéquation du référentiel de protection des données dans le pays cible (article 45 du RGPD)

- Garanties appropriées (article 46 du RGPD), notamment Binding Corporate Rules ou règles d'entreprise contraignantes (article 46. 2b, article 47), clauses type de protection des données adoptées par la Commission ou une autorité de contrôle
- Convention d'entraide judiciaire (article 48 du RGPD)
- Cas particuliers et exceptions (article 49 du RGPD)

3 Organisation

L'entreprise doit instaurer et entretenir une organisation qui, au regard de sa taille et à sa structure, permet la mise en œuvre des mesures nécessaires de protection des données à traiter et la stratégie annoncée. Cette organisation comprend notamment les ressources (financières et effectif) ainsi que les compétences nécessaires.

3.1 Organisation de la protection des données

Il s'agit d'assurer la sécurité et la régularité du traitement des données à caractère personnel et des données permettant d'identifier les personnes. Ce paragraphe n'aborde pas les différentes procédures spécialisées et ne préjuge pas du caractère approprié et efficace des dispositions en matière de protection des données.

3.1.1 Modalité d'organisation

L'organisation retenue correspond-elle à la stratégie adoptée ?

- Structuration nationale et internationale de l'entreprise
  - Existe-t-il un traitement des données à l'étranger ?
  - Existe-t-il une gestion appropriée des contrats avec :
    - les entreprises liées ?
    - les prestataires de services ?
  - Le service responsable du traitement est-il situé à l'étranger ?
- Existe-t-il des exigences locales/nationales particulières quant à la protection des données et à son organisation ?
- Mise en place de l'organisation de la protection des données
  - Existe-t-il une organisation centralisée/décentralisée de la protection des données ?
  - Existe-t-il une forme hybride ?

3.1.2 Lignes directrices relatives à la protection des données et à la sécurité des données

- L'instance dirigeante (direction générale ou directoire) a-t-elle fixé des lignes directrices relatives à la gestion de la protection des données et à la sécurité du traitement ?
- Ces instructions indiquent-elles l'importance de la protection des données et de la sécurité du traitement ? Définissent-elles des objectifs de protection ?
- Les objectifs de sécurité incluent-ils la confidentialité, l'intégrité et la disponibilité des systèmes ?
- Les objectifs de protection des données comprennent-ils la transparence, la portabilité et la traçabilité ?

3.1.3 Exigences concernant le délégué à la protection des données

- La conception de l'organisation de la protection des données tient-elle compte des exigences concernant le délégué à la protection des données, en particulier :
  - sa crédibilité
  - son indépendance
  - ses moyens
  - ses connaissances spécialisées
- Les responsabilités sont-elles clairement définies ?
- Comment le délégué à la protection des données a-t-il été désigné par le responsable de la protection des données (direction de l'entreprise) ?
  - D'autres délégués à la protection des données ont-ils été désignés (dans un réseau d'entreprises) ?
  - Des coordinateurs de la protection des données sont-ils nommés dans les unités opérationnelles ou les branches d'activité ?
- Le délégué à la protection des données est-il directement rattaché à la direction sans être soumis, dans l'exercice de ses activités, à aucune instruction de la direction générale et du management ? Existe-t-il une description des activités/tâches avec des attributions, des droits et des obligations clairs ?
- Le délégué à la protection des données accomplit-il ses tâches en fonction des risques ?
- Les activités de conseil et de surveillance du délégué à la protection des données sont-elles décrites et communiquées ?

- La répartition des tâches entre le délégué à la protection des données et les coordinateurs de la protection des données est-elle clairement définie en fonction de la forme d'organisation choisie ? Dispose-t-il des connaissances nécessaires ?
- Ses autres missions opérationnelles ne sont-elles pas en conflit avec son activité de délégué opérationnel à la protection des données de l'entreprise ?
- Existe-t-il un reporting régulier ? Comment est-il formalisé et étayé ?
- Un rapport annuel ou trimestriel est-il adressé à l'instance dirigeante (p.ex. direction générale, directoire) ?

3.2 Intégration de la protection des données dans les activités opérationnelles

Le délégué à la protection des données de l'entreprise contrôle notamment le respect du RGPD et des autres dispositions légales. Il a un rôle de conseil et d'appui pour la correction des défaillances identifiées. Le traitement de ces défaillances est formalisé et peut être vérifié de manière aléatoire dans le cadre d'audits internes.

- Le délégué à la protection des données est-il impliqué dans la planification et le contrôle de la mise en œuvre de mesures techniques et organisationnelles ?
- Les activités de surveillance ont-elles lieu régulièrement et en lien avec un événement donné ?
- Entretient-il des contacts réguliers avec l'autorité de contrôle compétente sur les questions de protection des données des salariés et de protection des données à caractère personnel des personnes concernées ?
- Le délégué à la protection des données réalise-t-il des actions régulières de sensibilisation et de formation (idéalement une combinaison de formations sur le lieu de travail et d'actions d'e-learning) ?

Afin d'attester de l'intégration de la protection des données dans les activités opérationnelles selon le RGPD, les mesures doivent être documentées par les 4 phases suivantes :

- Planification et conception
  - Y a-t-il une conception des processus automatisés basée sur une approche fondée sur les risques liés à la nature, l'ampleur, les circonstances et la finalité du traitement ?

- Mise en œuvre
  - Des mesures techniques et organisationnelles appropriées ont-elles été prises ? Les principes de protection des données dès la conception (« *privacy by design* » article 25.1 du RGPD) ou par défaut (« *privacy by default* » article 25.2 du RGPD) ont-ils été respectés ?
- Contrôle des résultats et surveillance
  - Les mesures ont-elles été ou sont-elles régulièrement vérifiées ?
- Optimisation et amélioration
  - Les mesures sont-elles régulièrement actualisées ?

3.3 Conditions générales d'utilisation des systèmes d'information

L'autorité responsable est tenue d'assurer la documentation nécessaire du traitement automatisé des données. Dans le choix de mesures de sécurité techniques et organisationnelles appropriées et la justification d'une mise en œuvre conforme aux exigences réglementaires et efficace, l'entreprise doit prendre en compte les instructions de l'Office fédéral allemand de la sécurité des technologies de l'information (Bundesamts für Sicherheit in der Informationstechnik, BSI), notamment celles définies dans les normes 100-1 à 100-3.[3]

- Le délégué à la protection des données valide-t-il le registre des activités de traitement conformément aux exigences du RGPD ?
- Le registre des activités de traitement peut-il être contrôlé à tout moment de façon aléatoire pour vérifier la pertinence et la documentation appropriée des questions mentionnées ?
- Le activités sous-traitées font-elles toutes l'objet d'un accord écrit lorsqu'elles concernent différentes procédures spécialisées ?
- Les accords font-ils partie de la documentation relative à l'utilisation des systèmes d'information ?
- Les modifications sur les systèmes informatiques ne sont-elles possibles que par les collaboratrices/collaborateurs explicitement autorisé(e)s ?
- Des mesures techniques et organisationnelles ont-elles été prises dans l'entreprise pour l'exécution des activités sur les systèmes répertoriés ?

[3] NdT: En France, l'ANSSI propose également une série de bonnes pratiques et de recommandations.

- Les mesures prises par l'entreprise pour la documentation des modifications sur les équipements, les programmes et les procédures du système d'information répondent-elles aux exigences du RGPD ?
- Les modifications sont-elles d'abord exécutées sur des systèmes test ? L'exécution des tests est-elle documentée par écrit ?
- Un responsable de la sécurité des SI (RSSI) a-t-il été nommé ?
- Les tâches du délégué à la sécurité informatique ont-elles été formellement définies ?
- Le délégué à la sécurité informatique est-il responsable de l'élaboration et de la révision de la conception des mesures de sécurité et du maintien du niveau de sécurité ?
- L'adoption des modifications de système se fait-elle en accord avec le délégué à la sécurité informatique ?

3.4 Adaptation de la structure organisationnelle au principe du guichet unique

Le principe du guichet unique est une nouveauté du RGPD. Cela signifie que, en cas de traitement transnational (défini à l'article 4.23 du RGPD), l'autorité de contrôle dite principale est l'unique interlocuteur du responsable ou du sous-traitant. Lors de l'adaptation de la structure organisationnelle, l'entreprise doit se baser sur les règles internes relatives à la sécurité informatique.

- Les interlocuteurs et la procédure de traitement, la documentation et le suivi des incidents de sécurité et de protection des données sont-ils définis dans les règles internes ?
- Les incidents de sécurité et de protection des données sont-ils couverts par une procédure spécialement définie à cet effet, y compris la gestion de crise et les rôles et responsabilités des délégués à la protection des données ou d'autres collaborateurs ?
- Les incidents de sécurité et de protection des données font-ils l'objet d'un suivi écrit, étant donné que l'autorité de contrôle peut vérifier, de manière aléatoire, la documentation sur place.
- Le délégué à la protection des données utilise-t-il des processus appropriés pour la mise en œuvre du devoir d'information en cas d'accès non autorisé aux données ?

Il incombe au délégué à la protection des données un rôle primordial quant au respect des délais prévus dans le RGPD. Afin de garantir le respect des devoirs du responsable du traitement et du sous-traitant lors de la notification à l'autorité de contrôle compétente, l'intégration du délégué à la protection des données dans les procédures internes appropriées de notification/information est obligatoirement nécessaire.

- A-t-on l'assurance que tous les processus soumis à notification peuvent être traités de manière centralisée conformément aux délais exigés (cf. chapitre 2 sur les règles et exigences) ?
- Existe-t-il des mesures de remédiation en cas de violation de la protection des données à caractère personnel (article 33, 34 du RGPD) ?

Pour les droits à l'information des personnes concernées, le délégué à la protection des données est à disposition pour conseiller et aider le département responsable du traitement à répondre.

- Le délégué à la protection des données vérifie-t-il régulièrement la mise en œuvre appropriée des mesures techniques et organisationnelles pour la rectification, la suppression et le blocage de données à caractère personnel ?

4 Communication et procédures

La principale condition de l'efficacité de la protection des données est une sensibilisation appropriée. Elle passe en particulier par des formations (information) et le conseil. Le respect des exigences doit être facilité par des procédures internes.

4.1 Communication sur les réglementations relatives à la protection des données

- Des séances de sensibilisation ou de formation (information et communication, contrôle des connaissances, attestation de formation, attestation et taux de participation, mise à jour régulière) ont-elles été/sont-elles proposées/réalisées ?
- Comment se déroule l'engagement à la confidentialité des données ? (Définition des catégories de personnes, auto-engagement, justification). Selon l'article 29 du RGPD, seules les personnes agissant sous l'autorité du responsable du traitement ou ses sous-traitants ne peuvent traiter des données à caractère personnel que sur instruction du responsable du traitement. Il en résulte la nécessité d'un accord ou d'un engagement entre les parties.

4.2 Adaptation des procédures internes au Règlement général de l'Union Européenne sur la protection des données

- Les accords d'entreprise existants sont-ils en accord avec le Règlement général sur la protection des données ? Il convient de vérifier dans quelle mesure les accords d'entreprise existants répondent aux exigences de l'article 88 du RGPD. Ils ne peuvent pas être en deçà du niveau de protection requis par le RGPD. Le périmètre et le contenu des accords d'entreprise correspondent aux exigences de l'article 88.1 et 88.2.
- Les déclarations de consentement existantes continuent-elles d'être effectives ?

En principe, les déclarations de consentement, selon l'article 4.11 du RGPD, n'ont plus à être fournies par écrit. Un consentement avisé et explicite suffit. Toutefois l'entreprise continue d'être tenue de produire la preuve du consentement donné, conformément à l'article 7. 1 du RGPD.

Il convient de vérifier si les déclarations de consentement répondent aux exigences suivantes :

- Langage clair et compréhensible
- Dissociation d'autres sujets
- Remise sans contrainte
- Accès facile
- Subordination selon l'article 7.4 du RGPD
- Révocabilité pour l'avenir
- Production du justificatif de l'existence d'un consentement

Lorsqu'un enfant âgé de moins de 16 ans doit donner son consentement, le responsable du traitement doit, en plus des points ci-dessus et conformément à l'article 8 du RGPD, s'assurer raisonnablement que le consentement est donné par le titulaire de la responsabilité parentale ou avec son accord.

- Y a-t-il sous-traitance et est-elle contrôlée ?
- Comment est-il assuré que la sous-traitance répond aux exigences de l'article 28 ?
- Le traitement se fait-il sur la base d'un contrat valide entre le responsable et le sous-traitant ? Les contenus minimaux de ce contrat sont définis à l'article 28.3 du RGPD.

Compte tenu de la responsabilité commune des responsables et du sous-traitant conformément à l'article 82 du RGPD, il convient également de vérifier dans quelle mesure l'entreprise elle-même agit comme sous-traitant.

- A-t-on l'assurance que l'entreprise tient un registre des activités de traitement conformément à l'article 30.2 du RGPD et a des procédures de notification fonctionnelles pour signaler sous 72 heures les violations de données à caractère personnel ?
- Existe-t-il des mécanismes de contrôle automatisés pour la détection d'utilisations abusives de données/pertes de données ?

4.3 Vérification des procédures relatives à la protection des données hors de l'entreprise

- Existe-t-il des activités sous-traitées à des fournisseurs externes ?
- Le cas échéant, des consentements existent-ils ?
- Comment sont traités les refus de consentement (publicité, communication) ?
- En cas de présence sur les réseaux sociaux, les processus sont-ils harmonisés avec le délégué/le responsable de la protection des données ?

4.4 Surveillance et adaptation permanente de la protection des données

- Comment le suivi général des messages d'erreur est-il organisé ?
- Les constats des contrôles précédents sont-ils pris en compte ?
- Existe-t-il des indicateurs clés de performance (KPI) de protection des données (par exemple pour les processus de certification) et comment sont-ils traités ?

4.5 Lignes directrices lors de demandes et de vérifications des autorités de contrôle de la protection des données

- Existe-t-il des lignes directrices (sont-elles actualisées) ?
- L'implication directe de l'organisation de la protection des données est-elle assurée ?
- La documentation relative aux demandes et au traitement peut-elle être produite ?

4.6 Lignes directrices en cas de demandes extérieures

- Existe-t-il une procédure concertée et des responsabilités définies au sein de l'organisation ?
- Comment l'implication directe de l'organisation de la protection des données (instruction en matière de procédure, description de processus, etc.) est-elle assurée ?

5 Reporting

Compte tenu de la responsabilité prévue à l'article 5.2 du RGPD, il est nécessaire de mettre en place un système de reporting approprié :

L'obligation de preuve concerne en particulier :

- la licéité du traitement ;
- la finalité du traitement ;
- la minimisation des données ;
- l'exactitude des données ;
- la suppression à temps des données ;
- l'intégrité et la confidentialité des données.

Le système de reporting doit se fonder sur les exigences relatives au registre des activités de traitement conformément à l'article 30 du RGPD.

Outre le compte-rendu régulier, le compte-rendu suscité par un motif (rapports ad-hoc) doit également être vérifié, en particulier en réaction à une demande de renseignement d'une personne concernée (article 15 du RGPD) ainsi qu'en réaction à une violation de la protection des données au sens des articles 32 et 33 du RGPD.

Le non-respect des obligations relatives à ces deux types de reporting peut entraîner des amendes de la catégorie la plus élevée (jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel).

5.1 Rapports réguliers légaux et reporting interne (p. ex. rapports d'activité)

5.1.1 Fréquence et périmètre des rapports

- Existe-t-il une note d'instruction, une procédure ou un document équivalent à propos de la fréquence des rapports, leur liste de diffusion et le responsable de leur réalisation et leur périmètre ?
- En l'absence d'une telle instruction, existe-t-il un historique suffisant attestant que les rapports sont régulièrement diffusés, selon un périmètre et un format cohérent ? En fonction de cet historique et de situations particulières (p. ex. démission du responsable, restructuration qui interrompt le flux d'information), une « procédure de fait » pourra être constatée.

5.1.2 Contenu des rapports

Le rapport régulier doit permettre au destinataire d'avoir l'assurance que les activités de protection des données répondent aux dispositions légales (et aux éventuelles exigences spécifiques à l'entreprise ou au secteur). A cet effet, le rapport doit a minima :

- énumérer tous les incidents au cours de la période couverte par le rapport et, le cas échéant, renvoyer à la documentation relative à ces incidents ;
- évoquer tous les changements significatifs dans le registre des activités de traitement au cours de la période couverte par le rapport ;
- contenir les statistiques concernant les demandes d'information et leur durée de traitement (ou à défaut, mention « néant ») ;
- actualiser les informations relatives au statut des projets liés à la protection des données ;
- faire apparaître les moyens mis à disposition pour la protection des données au cours de la période du rapport.

Si des rapports de fréquence et périmètre différents sont produits pour différents groupes de destinataires (internes, externes, commissaires aux comptes, instance représentative du personnel, direction informatique, société-mère, etc.), ces différences doivent suivre une logique compréhensible et être cohérentes pour des informations de nature et d'importance identiques.

Le périmètre attesté par la revue des précédents rapports peut remplacer la description formelle de la conception des rapports.

5.1.3 Documentation à l'appui des rapports

- Les derniers rapports répondent-ils aux exigences prévues ci-dessus ?
- Y a-t-il une vérification de l'exactitude et de l'exhaustivité des informations sur un exemple concret ?
- La traçabilité et la fiabilité des sources sont-elles évaluées ? Par exemple, tous les canaux de réception des demandes d'informations sont-ils vraiment pris en compte ou est-ce que les indicateurs correspondent au canal le plus fréquent de prise de contact ? Le rapport est-il effectivement parvenu à la liste de diffusion prévue ?
- Est-il possible d'attester sans vérification du contenu que, depuis l'entrée en vigueur du règlement, un rapport a effectivement été produit au cours de chaque période couverte par le rapport et distribué immédiatement à la fin de la période ?

5.2 Rapport motivé (rapport ad hoc) à l'autorité de contrôle de la protection des données et/ou à une instance interne

Le processus de production du rapport ad hoc devra démarrer dès que l'entreprise a connaissance d'une perte de données ou d'un traitement non autorisé ou illicite. De même, un tel événement ou une demande d'information au délégué à la protection des données doit également entraîner une réaction dans le délai prévu.

5.2.1 Aperçu des motifs potentiels d'incidents soumis à déclaration

- L'entreprise a-t-elle un aperçu de tous les motifs potentiels d'incidents soumis à déclaration ?
- Existe-t-il une description des scénarios d'incidents plausibles ? Qui collecte les informations concernant ces incidents ? Comment sont-elles transmises ?

- Outre les incidents, les demandes d'information des différents groupes de personnes concernées sont-elles également recensées (collaborateurs, clients, prospects, candidats, proches de clients/patients, tuteurs d'enfants, etc.) ?

5.2.2 Exigences locales

Une préparation appropriée à l'émission d'un rapport ad hoc peut consister à élaborer des instructions d'ordre général ou encore à constituer un recueil de modèles de rapport en fonction des situations.

- Existe-t-il des exigences locales concernant le rapport motivé ?
- Les exigences internes de notification sont-elles mises en œuvre, p. ex. mesures de remédiation ?

5.2.3 Documentation à l'appui des rapports ad hoc

- Le rapport pour des motifs concrètement connus était-il compréhensible ?
- Le rapport ad hoc correspond-t-il au périmètre attendu ?

Auteurs

Elaboré par le groupe de travail Audit interne & protection des données de l'IIA Allemagne

DIIR – Deutsches Institut für Interne Revision e.V.

Theodor-Heuss-Allee 108

60486 Frankfurt am Main

Contact : arbeitskreise@diir.de

Publié en octobre 2017 sur www.diir.de

Version 1.0

This document was translated in French by The IIA France in September 2018.

ISBN : 978-2-915042-94-8