Protection des données au niveau de l'audit interne

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.

Ce guide a été élaboré selon l'état actuel de la réglementation et des connaissances. Il ne prétend être ni obligatoire ni exhaustif et ne se substitue en aucun cas à la vérification de la situation juridique de chaque organisation.

Vous pouvez adresser vos remarques et commentaires à arbeitskreise@diir.de et pour la version française à recherche@ifaci.com.

1 La protection des données, une obligation légale 4

1.1 Législations allemande et européenne 4

1.2 Principes fondamentaux du RGPD 5

2 Importance de la protection des données au niveau de l'audit interne 6

2.1 Principes 6

2.2 Données à caractère personnel 8

2.3 Données des employés 8

2.4 Requêtes internes concernant les employés 9

3 Rôle du délégué à la protection des données 12

3.1 Position dans l'entreprise 12

3.2 Missions 13

3.3 Contexte international 14

4 Mise en oeuvre des dispositions légales relatives à la protection des données 15

4.1 Règles fondamentales 15

4.2 Préparation de la mission d'audit 17

4.3 Réalisation de la mission 18

4.4 Communication des résultats de la mission 19

4.5 Archivage des données de la mission 20

4.6 Lignes directrices en cas de demandes extérieures 19

1 La protection des données, une obligation légale

1.1 Législations allemande et européenne[1]

Le droit à l'autodétermination en matière d'information est le droit de chacun à déterminer soi-même la divulgation et l'utilisation de ses données personnelles. Il constitue la base des règlementations en matière de protection des données existantes en Allemagne. Pour l'essentiel, il s'agissait jusqu'à présent de la loi fédérale allemande de 1977 relative à la protection des données (*Bundesdatenschutzgesetz* (BDSG)) et des réglementations régionales[2] et sectorielles[3].

Toutes les entreprises opérant en Europe sont touchées par les importantes répercussions du Règlement général européen sur la protection des données (RGPD), entré en vigueur en mai 2018. Avec le RGPD, le droit relatif à protection des données doit continuer d'être harmonisé au niveau européen et modernisé compte tenu des évolutions technologiques actuelles. A partir du 25 mai 2018, il est applicable immédiatement dans les Etats membres de l'UE et modifie ainsi les réglementations nationales existantes comme la loi fédérale allemande relative à la protection des données en vigueur (BDSG).

Des clauses de flexibilité permettent aux différents Etats membres de régir certains aspects supplémentaires de la protection des données dans leur législation nationale. Ainsi la législation allemande a été complétée et révisée par la loi fédérale allemande relative à l'adaptation et à la mise en œuvre de la protection des données (*Datenschutz-Anpassungs- und Umsetzungsgesetz-EU* (DSAnpUG-EU)). Celle-ci reprend la BDSG révisée et modifie également d'autres lois existantes.

---

[1] 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] En Allemagne, les lois régionales relatives à la protection des données sont valables, jusqu'à leur remplacement par le RGPD au plus tard en mai 2018, pour les différentes autorités régionales et administrations communales et éventuellement en complément de réglementations spécifiques.

[3] Ces réglementations spécifiques sont adaptées aux exigences des différents secteurs et priment, en principe, sur les règles générales de la loi fédérale allemande relative à la protection des données (BDSG). En particulier, pour les organisations qui traitent des données (articles 67 et suivants du *Sozialgesetzbuch X*), les organisations du secteur des télécommunications (articles 91 et suivants de la *Telekommunikationsgesetz*, articles 11 et suivants de la *Telemediengesetz*), et les organisations religieuses (*Kirchliche Datenschutzordnung* et *Datenschutzgesetz der Evangelischen Kirche Deutschland*).

Après l'entrée en vigueur du RGPD et des lois complémentaires, d'autres précisions pour la mise en œuvre pratique des nouveaux règlements sont encore attendues comme, par exemple, les notes d'interprétation et d'instruction émises par les autorités de contrôle. Il faut prévoir la même démarche pour les réglementations régionales et sectorielles.

Ce guide met l'accent sur les dispositions du RGPD et de la loi fédérale allemande révisée relative à la protection des données pertinentes pour les travaux de l'audit et met en évidence les principaux impacts concrets dans le processus d'audit interne.

1.2 Principes fondamentaux du RGPD

Les données à caractère personnel doivent, conformément au RGPD, répondre à certains critères fondamentaux[4] :

- traitées de manière licite, loyale et transparente pour la personne concernée (« licéité, loyauté, transparence ») ;
- collectées uniquement pour des finalités déterminées (« finalité ») ;
- adéquates, pertinentes et limitées à ces finalités (« minimisation des données ») ;
- exactes et, lorsque ce n'est pas le cas eu égard aux finalités du traitement, effacées ou rectifiées sans tarder (« exactitude ») ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités du traitement (« limitation de la conservation ») ;
- traitées de façon à garantir une sécurité appropriée, y compris la protection contre le traitement non autorisé, la perte, la destruction ou les dégâts d'origine accidentelle à l'aide de mesures techniques ou organisationnelles appropriées (« intégrité et confidentialité »).

Le responsable du traitement[5] doit être en mesure de démontrer que celui-ci est respecté (responsabilité[6]).

[4] Les principes sont énumérés à l'article 5 du RGPD et expliqués au considérant 39.

[5] La notion de « responsable du traitement » est définie à l'article 4.7 du RGPD.

[6] Article 5.2 du RGPD.

2 Importance de la protection des données au niveau de l'audit interne

2.1 Principes

Les réglementations en matière de protection des données doivent être respectées dès lors que des données à caractère personnel sont en jeu. En principe, le droit relatif à la protection des données n'est pas un droit absolu[7]. Certaines questions ne sont pas explicitement réglementées. Elles nécessitent une décision au cas par cas qui met en balance les intérêts de l'organisme qui traite les données au regard des intérêts des personnes concernées (principe de proportionnalité).

Les données à caractère personnel sont souvent en relation avec des processus métiers. Le nombre sans cesse croissant de transactions et de fichiers de données ainsi que l'utilisation des systèmes d'information dans presque tous les domaines opérationnels font que ces données peuvent être systématiquement examinées et exploitées en grandes quantités.

Les tests de l'audit interne sont donc de plus en plus fréquemment liés au traitement et à l'utilisation de données à caractère personnel ou susceptibles de permettre l'identification de salariés ou de tiers (p. ex. partenaires commerciaux ou clients). Des documents et données (dossiers, fichiers, e-mails) provenant des systèmes de gestion sont consultés, exploités et fusionnés.

Leur simple présence dans les systèmes ne justifie pas que les entreprises puissent disposer de ces données à leur convenance. Ainsi, chaque traitement de données à caractère personnel doit être réalisé sur la base d'un but légitime. En raison du rôle de l'audit interne, la finalité du traitement dans le cadre des missions peut se justifier dans le cadre des réglementations relatives à la protection des données. L'audit interne dispose d'un droit d'accès illimité à l'information[8]. Ce droit vaut pour la consultation et l'exploitation des données nécessaires à l'accomplissement de ses missions, pour autant que les dispositions relatives à la protection des données soient respectées.

En Allemagne, les fondamentaux et les exigences en matière de protection des données à l'égard du traitement des données à caractère personnel sont restées

[7] NdT: considérant 4, principe de proportionnalité.

[8] Cf. Normes de l'IIA 1000 (Mission, pouvoirs et responsabilités) et 1130 (Atteinte à l'indépendance ou à l'objectivité).

inchangés avec le RGPD. Le principe selon lequel tout traitement de données à caractère personnel nécessite une autorisation est repris dans le RGPD. L'article 6 du RGPD liste les conditions de validité du traitement. Ainsi, outre le consentement de la personne concernée, la licéité peut notamment résulter de :

- l'exécution d'un contrat ou de mesures précontractuelles ;
- l'accomplissement d'une obligation légale ;
- l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ;
- les intérêts légitimes du responsable du traitement après mise en balance des intérêts ou des libertés et droits fondamentaux de la personne concernée.

La licéité du traitement et de l'utilisation des données dans le cadre de l'activité de contrôle et de surveillance de l'audit interne résulte en règle générale de l'article 6. 1. f du RGPD (défense des intérêts légitimes).

> *L'article 6.1.f du RGPD exige une pondération des intérêts légitimes de l'entreprise par rapport aux intérêts des personnes concernées qui exigent une protection des données à caractère personnel. Dans ce cadre, il est recommandé d'impliquer très tôt le délégué à la protection des données pour discuter de la procédure générale (cf. chapitre 3 sur le Rôle du délégué à la protection des données).*
>
> *La licéité d'un traitement nécessaire au respect d'une obligation légale indiquée à l'article 6 du RGPD, signifie que des dispositions légales prioritaires justifient le traitement des données concernées*[9].

Le RGPD a un domaine d'application géographique. Concernant l'activité de l'audit interne, il s'applique toujours lorsque le service d'audit est établi dans l'Union européenne, que le traitement des données ait lieu dans l'Union européenne ou non.

[9] Cf. considérant 45 du RGPD.

2.2 Données à caractère personnel

Une donnée est à caractère personnel dès qu'elle se réfère à une personne physique précise ou que celle-ci peut être directement ou indirectement identifiée. Est considérée comme personne physique identifiable, une personne qui peut être identifiée directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale[10].

Dans le cas des activités d'audit, ces critères sont souvent remplis. Les saisies de données clients dans les systèmes, les noms sur les justificatifs, les relevés de comptes ou les contrats ainsi que les identifiants, les numéros personnels et les données sur les salaires nécessitent le respect des dispositions relatives à la protection des données lors de leur utilisation dans une mission d'audit.

Lorsqu'une référence aux personnes n'est pas nécessaire ou que les travaux sont effectués avec des données anonymisées (c'est-à-dire des données dont la référence aux personnes a été retirée), il n'y a pas lieu d'appliquer les règles sur la protection des données.

Un exemple typique est une analyse de justificatifs sans lien avec les données des collaborateurs du service comptable ou d'autres personnes concernées dans cette analyse.

2.3 Données des employés

Le RGPD ne contient aucune liste spécifique d'autorisations pour le traitement des données des salariés. La protection des données des employés fait partie des paragraphes du RGPD qui prévoient une réglementation ou une précision nationale. Des dispositions spécifiques pour la protection des données dans la relation employeur-employé peuvent être établies par des lois ou des conventions collectives (article 88 du RGPD et aussi article 26.4 de la loi fédérale allemande révisée relative à la protection des données). Ainsi, le traitement des données peut continuer de s'appuyer sur les conventions collectives et autres accords propres à l'entreprise.

[10] Article 4.1 du RGPD.

Dans la relation employeur-employé, ce sont les conditions générales du RGPD qui s'appliquent d'abord. Selon la situation, différentes dispositions légales entrent en ligne de compte. Les procédures de traitement nécessaires à l'accomplissement du contrat de travail sont basées sur l'article 6.1.b du RGPD (exécution d'un contrat). Le traitement de données médicales dans la relation employeur-employé se base sur l'article 9 du RGPD qui vise le traitement des catégories particulières de données à caractère personnel (sensibles). Pour les traitements dans le cadre de l'activité de contrôle et de surveillance de l'audit interne, c'est de nouveau la sauvegarde des intérêts légitimes selon l'article 6.1.f du RGPD qui entre d'abord en ligne de compte en tant que base légale.

Dans la loi fédérale allemande révisée relative à la protection des données, l'article 26 est déterminant pour le traitement des données dans le contexte de l'emploi. La disposition précise et complète les prescriptions du RGPD, sans être en contradiction avec elles. L'article 26 reprend clairement les structures et réglementations essentielles de l'article 32 de l'ancienne loi de 1977. Ici aussi, il faut faire la part entre les intérêts légitimes de l'entreprise et ceux des employés.

> *Les données à caractère personnel des employés peuvent être traitées aux fins de la relation employeur-employé, lorsque cela est nécessaire à la décision de l'instauration d'une relation d'emploi ou après la formalisation de la relation d'emploi pour son accomplissement ou sa cessation ou pour l'exercice ou le respect des droits résultant d'une loi ou d'une convention collective, d'un accord d'entreprise et des droits et obligations relatifs à la représentation des intérêts des employés.*

Le traitement des données des employés est donc autorisé lorsqu'il est adapté aux fins de la relation employeur-employé, qu'il est le moyen le moins restrictif immédiatement effectif (nécessité) à disposition de l'entreprise et ne prévaut pas sur les intérêts des employés qui nécessitent une protection de leurs données à caractère personnel. Pour plus d'indications, se référer au chapitre 4.

2.4 Requêtes internes concernant les employés

Il en va autrement lorsque les données à caractère personnel d'employés doivent être traitées pour la détection d'infractions. Cela n'est autorisé qu'à certaines conditions. Plus particulièrement, des indices réels doivent justifier la suspicion d'une infraction dans la relation employeur-employé. Le terme de suspicion s'entend au sens juridique. Selon le niveau de soupçon et pour la distinguer de simples suppositions, le droit allemand identifie trois catégories de suspicion :

Suspicion initiale

Eventualité de commission d'un acte qui repose sur des preuves ou des indices selon lesquels quelqu'un a commis une infraction. Dans le cas de la suspicion initiale, les autorités policières ont le devoir d'ouvrir une procédure d'enquête.

Présomption suffisante de culpabilité

Probabilité que le suspect ait commis un acte délictueux et soit condamné. Ici, le parquet a le devoir de mise en accusation.

Présomption sérieuse

Forte probabilité que le suspect ait commis un acte délictueux. Les éléments à charge doivent prévaloir sur les éléments à décharge. Certaines actions sont alors légales, p.ex. détention préventive (article 112 du Code de procédure pénale allemand).

Les enquêtes à l'occasion de possibles actes frauduleux[11] se différencient essentiellement des missions classiques sur les processus opérationnels ou d'autres enjeux par le fait que, justement, les données à caractère personnel sont utilisées pour l'instruction des faits et que les conclusions concernent une ou des personnes précise(s). Il en découle des exigences particulières quant à l'obligation de diligence et la confidentialité dans la réalisation de la mission. L'implication du délégué à la protection des données, de l'instance représentative du personnel, ainsi qu'éventuellement du service juridique est alors requise, de même qu'une formalisation et une traçabilité particulières.

Les conditions pour le traitement des données des employés à l'occasion de la détection d'infractions résultent de l'article 26.1.2 de la loi fédérale allemande révisée relative à la protection des données :

- preuves et soupçon avéré d'une infraction
- infraction dans la relation employeur-employé
- nécessité de collecter des données pour la détection d'une infraction
- protection des employés et proportionnalité (pondération des intérêts d'investigation de l'entreprise et de la protection des droits individuels de la personne concernée)

[11] Selon le glossaire des Normes de l'IIA, la fraude désigne tout acte illégal caractérisé par la tromperie, la dissimulation ou la violation de la confiance sans qu'il y ait eu violence ou menace de violence. Les fraudes sont perpétrées par des personnes et des organisations afin d'obtenir de l'argent, des biens ou des services, ou de s'assurer un avantage personnel ou lié à leur activité.

Pendant la mission, la licéité des analyses doit être documentée en permanence pendant la durée de l'enquête et en particulier lors de la préparation de la mission et sa réalisation. Le respect de la proportionnalité et de la protection des intérêts légitimes doit être régulièrement évalué au cours de la mission et étayé par des preuves dans les documents de travail.

3 Rôle du délégué à la protection des données

3.1 Position dans l'entreprise

Selon le RGPD (art. 37.1 du RGPD)[12], organismes publics ou les entreprises traitant des données particulièrement sensibles. Toutefois, les Etats membres conservent le pouvoir d'adopter des réglementations complémentaires.

Ainsi, en Allemagne, l'obligation de désignation d'un délégué à la protection des données existait déjà et a été précisée par l'article 38 de la loi fédérale révisée qui la prévoit pour les responsables du traitement employant au moins 10 personnes en permanence pour le traitement automatisé de données à caractère personnel. Indépendamment de l'effectif, un délégué à la protection des données doit être désigné dès lors que les traitements effectués sont soumis à une analyse d'impact au sens de l'article 35 du RGPD.

Le responsable du traitement doit veiller à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données. Il doit lui fournir les ressources nécessaires, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettre de maintenir ses connaissances spécialisées[13]. Le responsable du traitement doit veiller à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions.[14]

> *Le délégué à la protection des données peut en principe accomplir d'autres missions et tâches dans la mesure où celles-ci n'entraînent pas de conflit d'intérêts[15]. Une activité supplémentaire en audit interne est certes possible en principe, toutefois il doit être garanti que les missions et responsabilités respectives n'entraînent aucun conflit d'intérêts (art. 38.6 du RGPD et norme internationale pour la pratique professionnelle de l'audit interne 1112 - Rôles du responsable de l'audit interne en dehors de l'audit interne). Pour cela, une séparation claire des tâches entre activités relevant de l'audit interne et celles concernant la protection des données sera utile.*

---

[12] cf. articles 37 à 39 du RGPD. Cette exigence vaut notamment lorsque l'activité principale de traitement des données à caractère personnel est effectuée à des fins de surveillance ou concerne des catégories particulières de données (par ex. de données médicales).

[13] Articles 38.1 et 38.2 du RGPD.

[14] Article 38.3 du RGPD.

[15] Cf. article 38.6 du RGPD selon lequel le responsable du traitement veille à ce que les autres missions et tâches du délégué à la protection des données n'entraînent aucun conflit d'intérêts.

Pour ce qui est des groupes d'entreprises, le RGPD (cf. article 37.2) indique qu'un seul délégué à la protection des données peut être désigné à condition que cette personne soit facilement joignable à partir de chaque lieu d'établissement.

3.2 Missions

Les missions et responsabilités du délégué à la protection des données sont régies à l'article 39 du RGPD. Il doit notamment :

- informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur leurs responsabilités en matière de protection des données ;
- contrôler (« monitor ») :
  - le respect du RGPD et d'autres réglementations en matière de protection des données ;
  - le respect des règles internes de protection des données, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, les « audits » s'y rapportant ;
- dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35 du RGPD ;
- coopérer avec l'autorité de contrôle ;

En principe, pour toutes les programmes de travail où des données à caractère personnel sont traitées, il convient de prévoir une coordination avec le délégué à la protection des données. Cela concerne notamment :

- l'introduction d'un outil informatisé d'audit ou des modifications significatives dans des outils existants ou d'autres programmes de travail traitant des données à caractère personnel ;
- le classement, la conservation et la suppression de données de l'audit interne ;
- les étapes clés du programme de travail (p. ex. analyses de données et accès temporaires aux systèmes, etc.) ;
- les procédures concernant la détection et l'investigation de situations suspectes ;
- les questions spécifiques soulevées lors de certaines missions.

3.3 Contexte international

De façon comparable aux dispositions de la loi fédérale allemande révisée relative à la protection des données, d'autres réglementations fixent des exigences locales qu'il convient, le cas échéant de respecter. Par exemple, le RGPD donne la possibilité aux Etats membres de préciser les critères de désignation d'un délégué à la protection des données.

Dans les entreprises ayant un siège social aussi bien à l'intérieur qu'à l'extérieur de l'Union européenne, il est recommandé de recourir à des experts locaux. Dans le cadre de la mise en œuvre du RGPD, les conditions d'accès des autorités de contrôle, des parties prenantes externes et des collaborateurs devraient être systématiquement analysées par le responsable du traitement.

4 Mise en œuvre des dispositions légales relatives à la protection des données

4.1 Règles fondamentales

L'audit interne doit déterminer des règles claires pour le traitement des données à caractère personnel. Par conséquent, les processus et le fonctionnement de l'audit interne doivent prendre en compte et respecter les règles relatives à la protection des données. Les auditeurs internes doivent être régulièrement formés et sensibilisés à ce sujet.

Le nouveau cadre légal a accru les exigences de conformité lors de la conception des programmes de travail. Certes, le principe de « protection des données dès la conception/par défaut » *(« privacy by design/privacy by default »)*[16] n'est pas nouveau ; il précise l'impératif déjà connu de la minimisation des données. L'article 25 du RGPD explicite cette obligation de mettre œuvre, dès la conception des moyens du traitement et tout au long de leur cycle de vie, des mesures techniques et organisationnelles nécessitant peu de données et avec des pré-configurations les plus respectueuses possibles de la protection des données. De plus, le RGPD exige une documentation suffisante prouvant que les exigences de protection des données ont été effectivement identifiées et efficacement appliquées.

Si l'audit interne utilise ses propres systèmes ou programmes pour le traitement et l'utilisation des données à caractère personnel, ceux-ci, y compris les mesures techniques et organisationnelles nécessaires, conformément à l'article 32.1 du RGPD et à l'article 64 de la loi fédérale allemande révisée relative à la protection des données, sont soumis aux suivis dont le délégué à la protection des données a la responsabilité[17]. Ils doivent être enregistrés dans le registre des activités de traitement prévu à l'article 30 du RGPD et être portés à la connaissance du délégué à la protection des données.

Conformément au RGPD, seules des mesures proportionnées doivent être mises en œuvre. L'article 32 du RGPD prévoit les éléments à prendre en compte lors de l'examen de la proportionnalité, à chaque fois en fonction des circonstances précises liées à

---

[16] « *Privacy by Design* » désigne la prise en compte des mesures techniques et organisationnelles garantissant la protection des données et la vie privée dès la conception du traitement. « *Privacy by Default* » désigne les pré-configurations respectueuses de la protection des données du point de vue de l'utilisateur.

[17] Si les données à caractère personnel des salariés de l'audit interne sont traitées (par exemple, l'affectation à des missions d'audit, l'identification, la gestion et la facturation des dépenses), la licéité de ce traitement s'appuie sur l'article 26.1 de la loi fédérale allemande révisée sur la protection des données (cf. 2.3).

chaque situation, notamment compte tenu de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques liés à la protection des données, dont le degré de probabilité et de gravité varie.

L'article 32 du RGPD est plus complet que l'article 9 de l'ancienne loi fédérale allemande relative à la protection des données, puisqu'il prévoit :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Selon le RGPD, pour définir les mesures de sécurité nécessaires, il faut d'abord constater le besoin de protection, ensuite évaluer les risques, prendre des mesures proportionnées et fournir des preuves. Le règlement suppose donc qu'une gestion de la sécurité informatique est mise en œuvre dans l'entreprise[18].

En comparaison avec la loi précédente, l'article 64 de la loi allemande révisée[19] cite de nouveaux contrôles liés à la protection des données, notamment en termes d'intégrité, de fiabilité et de restauration des données. D'autres aspects ont été reformulés ou déplacés : le contrôle des destinataires réels ou potentiels des données transmises, le contrôle lors de la transmission des données et du transport des supports de données, le contrôle de la conservation et le contrôle de l'utilisation par les personnes autorisées[20]. Conformément au premier alinéa de cet article, le responsable du traitement tient compte des instructions applicables et des recommandations de l'Office fédéral allemand de la sécurité des technologies de l'information (*Bundesamt für Sicherheit in der Informationstechnik* ou BSI) lors de la mise en œuvre de ces mesures.

---

[18] Cf. Gola/ Jaspers/ Müthlein/ Schwartmann « *Datenschutz-Grundverordnung im Überblick*", », 1ère édition 2017, p. 58

[19] L'article 64 de la loi fédérale allemande révisée sur la protection des données (« Exigences quant à la sécurité du traitement des données ») contient un aperçu avec la description des différents contrôles (au total 14).

[20] Cf. article 29 de la Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680&qid=1533113783256&from=DE

4.2 Préparation de la mission d'audit

Dès le lancement de la mission d'audit, il faut veiller à préciser les contenus pertinents en matière de protection des données au niveau des objectifs de l'audit, des risques identifiés et des procédures d'audit. Selon la mission d'audit, il peut y avoir une concertation avec le délégué à la protection des données. Cette précaution ne doit pas se limiter aux missions concernant les ressources humaines. Le délégué à la protection des données n'a pas le pouvoir de donner des instructions à l'audit interne, mais peut orienter la conformité de la mission d'audit vis-à-vis de la protection des données.

Il convient d'être particulièrement attentif aux considérations en matière de protection des données lors d'une mission portant sur des processus opérationnels ou dédiée à la protection des données.

Pour les audits incluant des données à caractère personnel, la mission d'audit doit préciser

- dans quel but les données sont utilisées ;
- quelles données sont prises en compte (p. ex. en particulier les données sensibles comme les données médicales ou les salaires) ;
- si l'objectif prévu ne peut être précisément atteint que par les données visées (pertinence et nécessité) ;
- quelles procédures alternatives existent éventuellement et seraient moins contraignantes à l'égard des droits individuels des personnes concernées (adéquation) ;
- si la protection des intérêts d'une personne concernée priment sur l'accomplissement de l'activité d'audit (proportionnalité).

L'analyse de ces critères et de leurs éventuelles modifications est appréciée au regard des intérêts en jeu.

Dans certains cas particuliers, il peut être nécessaire de faire appel à des prestataires externes pour des tests ou analyses spécifiques. Si le prestataire a alors la possibilité d'accéder ou de consulter les données à caractère personnel, il est nécessaire d'impliquer le délégué à la protection des données. Dans ce cas, il convient généralement de tenir compte des règles internes en matière de sous-traitance.

Pour les accès inter-sociétés ou les requêtes de données, il faut convenir par écrit ou sous une autre forme appropriée (p. ex. workflow électronique) de l'utilisation des données à caractère personnel avec les sociétés faisant l'objet de la mission d'audit. En pratique, cela peut être signalé dès l'annonce de la mission à la société concernée qui doit avoir la possibilité de vérifier dans un délai raisonnable si les réglementations locales ou régionales spécifiques ne s'y opposent pas.

4.3 Réalisation de la mission

La mission doit être réalisée selon un périmètre défini et en respectant les règles techniques et organisationnelles dans les procédures de la fonction d'audit interne.

Selon le principe de minimisation, il convient de traiter aussi peu de données à caractère personnel que possible à cette occasion. En particulier, celles-ci doivent être anonymisées ou pseudonymisées dans la mesure du possible selon la finalité d'utilisation et sans que des efforts disproportionnés par rapport à l'objectif de protection recherché ne soient nécessaires.

> *Lors de l'anonymisation, les données à caractère personnel sont modifiées de telle sorte qu'elles ne puissent plus être associées à une personne. Par contre, avec les données pseudonymisées, il continue d'être possible de remonter aux personnes concernées (p. ex. par des combinaisons de chiffres ou de lettres). En pratique, il est souvent difficile de mettre en œuvre l'anonymisation.*
>
> *Si la pseudonymisation est effectuée par l'audit interne lui-même en tant qu'utilisateur de données, il est à nouveau possible de remonter à tout moment aux données d'origine. Ainsi, dans le cas d'importantes collectes de données, l'identification d'une personne précise est possible malgré la pseudonymisation. Afin d'empêcher toute déduction, il faut éventuellement séparer ou modifier les données. En particulier, dans les entités de moins de 5 salariés, il est éventuellement possible de remonter jusqu'aux différentes personnes.*
>
> *Si, malgré la demande de l'audit interne, les données des services opérationnels arrivent non anonymisées ou pseudonymisées, il faut pouvoir y remédier au sein du service d'audit (voire d'une équipe d'auditeurs internes dédiée).*

Pour répondre à des exigences d'autres entreprises ou pour anticiper celles qui pourraient être requises pour sa propre entreprise, il peut être nécessaire dans des cas spécifiques d'exploiter les documents à caractère personnel (par exemple les e-mails) ou de les mettre à disposition. Si l'audit interne est impliqué dans ce processus, une concertation appropriée avec le délégué à la protection des données de ces entreprises devra être envisagée en tenant compte des dispositions légales applicables. Il est recommandé de documenter le résultat de la concertation.

4.4 Communication des résultats de la mission

Les résultats d'une mission d'audit sont généralement formalisés dans le rapport d'audit. Il contient les constats résultant des contrôles effectués, les évaluations des risques et les actions ou recommandations pour maîtriser les risques identifiés. Les rapports d'audit interne sont confidentiels. En cas de besoin, un niveau particulier de confidentialité peut être défini.

Le traitement approprié des résultats confidentiels et des rapports est à signaler au sein de la fonction d'audit interne et, le cas échéant, à d'autres salariés ou prestataires impliqués (par exemple, les commissaires aux comptes, les conseillers ou prestataires en matière de services informatiques). A cette occasion, il faut faire signer un accord de confidentialité, en particulier aux personnes extérieures.

La nature et l'ampleur de la diffusion du rapport sont à déterminer par la direction de l'audit interne, éventuellement en accord avec la direction de l'entreprise. Il en va de même pour la transmission en dehors de la liste de diffusion.

Dans des cas précis, les rapports d'audit peuvent contenir des données à caractère personnel ou permettant d'identifier des personnes ainsi que des informations confidentielles. En principe, les constats, actions ou recommandations ne sont pas reliés à des personnes précises, mais à des services ou unités. Toutefois, dans de petites entreprises ou unités, l'identification des personnes visées peut tout à fait être effectuée. Dans ces cas, il faut envisager des mesures de protection adaptées. Cela vaut aussi lorsque des données à caractère personnel font elles-mêmes partie des résultats de la mission.

Les résultats du suivi des actions correctrices et les documents associés sont à traiter comme les rapports d'audit.

4.5 Archivage des données de la mission

L'archivage des données de la mission (par exemple, les documents de travail et e-mails) doit respecter les règles en matière de protection des données des différentes lois. En théorie, le principe de subsidiarité qui donne la priorité aux directives légales spécifiques s'applique en matière de prescriptions sur la protection des données.[21]

A l'expiration des exigences légales et pour les documents sans pertinence opérationnelle ou fiscale, les dispositions en matière de protection des données doivent être respectées dans les cas où des données à caractère personnel ont été stockées. Pour cela, des règles relatives à l'effacement des données doivent être définies.

Lors de l'archivage de données à caractère personnel, le principe de minimisation s'applique. C'est-à-dire que la référence à la personne, dans la mesure où elle n'est pas obligatoirement nécessaire, doit être effacée et les données doivent être anonymisées. De plus, le principe de minimisation des données signifie aussi que les données, qui ne doivent plus être utilisées et conservées, sont bloquées et effacées.

[18] En Allemagne, les règles juridiques prioritaires concernant l'archivage sont notamment: en droit commercial : §§ 257, 261 HGB und Grundsätze ordnungsmäßiger Buchführung (GOB) ; Grundsatz des Institutes der Deutschen Wirtschaftsprüfer (IDW) RS FAIT 3 (Grundsätze ordnungsgemäßer Buchführung beim Einsatz elektronischer Archivierungsverfahren) ; en droit fiscal : §§ 146, 147, 200 AO, Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), § 14b Absatz 1 Satz 2 UStG, Abschnitt 14b.1. Umsatzsteuer-Anwendungserlass (UStAE) und diverse BMF-Schreiben ; en droit civil (en particulier concernant l'exploitabilité judiciaire) : §§ 415 ff. ZPO

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

Copyright © 2018 No parts of this material may be reproduced in any form without the written permission of The IIA Germany. Permission has been obtained from the copyright holder Deutsches Institut für Interne Revision e.V. Theodor-Heuss-Allee 108 - 60486 Frankfurt am Main to publish this translation, which is the same in all material respects, as the original unless approved as changed. No parts of this document may be reproduced, stored in any retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of The IIA Germany.

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

ISBN : 978-2-915042-95-5