_swissprivacy.law

Dossier médical du salarié consulté par l'employeur : jusqu'où va la souplesse du RGPD ?

Anna Ploix, le 3 juillet 2025

Une supérieure hiérarchique accède au dossier médical d'une employée avant de la licencier. L'autorité de protection des données tranche : l'employeur n'est pas responsable, l'absence de notification de la violation ne lui est pas reprochée. Une décision qui interroge les fondements mêmes de la responsabilité de l'employeur.

Décision 64/2025 de l'Autorité de protection des données (Belgique) du 1er avril 2025

Faits

Une employée, licenciée par une association hospitalière, apprend que sa supérieure hiérarchique a consulté son dossier médical la veille de la notification de son licenciement. Elle introduit une plainte devant l'Autorité de protection des données belge (Gegevensbeschermingautoriteit) alléguant une violation du RGPD, notamment au regard du défaut de notification de cette violation (art. 33 RGPD). La décision est finalement rendue par la Chambre Contentieuse le 1er avril 2025.

L'Association Hospitalière admet la consultation fautive, mais soutient que la supérieure a agi de sa propre initiative, sans instruction de sa part. Une procédure disciplinaire est ouverte à l'encontre de la supérieure, mais aucune notification de la violation n'est effectuée auprès de l'autorité de contrôle.

Responsable de traitement : dissociation hiérarchique et qualification autonome

L'une des principales contributions de cette décision réside dans la qualification juridique opérée par la Chambre Contentieuse quant à la notion de responsable du traitement, lorsqu'un salarié, en l'occurrence une supérieure hiérarchique, accède de manière illicite à des données sensibles. En l'espèce, la Chambre considère que la supérieure hiérarchique a agi non pas au nom de son organisation, mais en tant que responsable autonome du traitement au sens de l'art. 4 par. 7 RGPD, dans la mesure où elle aurait déterminé seule les finalités et les moyens du traitement en cause, à savoir la consultation du dossier médical d'une subordonnée à la veille de son licenciement.

Cette analyse repose sur une série d'éléments factuels que la Chambre estime décisifs. Elle relève notamment que la consultation du dossier s'est produite en dehors des heures habituelles de travail, qu'aucune instruction n'avait été donnée par l'association hospitalière et que la supérieure a reconnu avoir agi de sa propre initiative, motivée par le souci d'évaluer la capacité psychologique de la plaignante à recevoir la nouvelle de son licenciement. Ce faisant, la Chambre conclut que l'intéressée a agi en dehors du périmètre d'autorité qui lui était confié, en détournant à des fins personnelles une prérogative professionnelle, ce qui justifierait l'exclusion de la responsabilité de l'employeur.

Cette position, bien qu'en apparence conforme aux lignes directrices du Comité européen de la protection des données (CEPD), soulève des difficultés d'ordre systémique. En effet, il est généralement admis que lorsqu'un salarié traite des données dans le cadre de son activité professionnelle, ce traitement est réputé être effectué sous l'autorité de l'organisation, sauf à démontrer une rupture manifeste dans le lien de subordination ou un détournement tel que le traitement ne puisse raisonnablement être rattaché aux finalités poursuivies par l'entité. Or, dans une structure hospitalière où l'organisation conserve la maîtrise des accès, des habilitations et des dispositifs de contrôle interne, il peut paraître excessivement formaliste d'écarter sa qualité de responsable au motif que la consultation incriminée n'a pas été expressément commandée ou autorisée. Une telle lecture pourrait conduire à fragiliser le principe même d'imputabilité du responsable du traitement, en ouvrant la voie à une segmentation de la responsabilité fondée sur des appréciations subjectives de l'intentionnalité des acteurs.

En outre, une telle dissociation pourrait avoir pour effet de restreindre la portée de la protection offerte aux personnes concernées. En écartant l'employeur du champ de la responsabilité, le justiciable se voit privé de la possibilité de soulever à son encontre les obligations incombant au responsable du traitement au titre des art. 24 et 32 du RGPD, en matière de prévention, de contrôle et de réaction aux incidents. La responsabilité du supérieur hiérarchique, en tant que personne physique, reste en pratique difficile à mettre en œuvre, notamment en raison de l'absence d'assise organisationnelle, de moyens financiers ou d'obligations procédurales équivalentes à celles d'une personne morale.

La qualification retenue par la Chambre, si elle permet d'individualiser la faute et de souligner le caractère déviant du comportement de la supérieure, s'écarte donc d'une approche fondée sur la responsabilité structurelle de l'employeur.

Violation de données : absence de notification malgré la sensibilité des données

La seconde question centrale abordée par la Chambre Contentieuse concerne l'absence de notification à l'autorité de contrôle d'un accès non autorisé à des données de santé, en l'espèce le dossier médical d'une employée. La Chambre reconnaît sans équivoque qu'il y a eu une violation de données à caractère personnel au sens de l'art. 4 par. 12 RGPD, dès lors que la supérieure hiérarchique a accédé de manière non autorisée à des données de santé, lesquelles relèvent d'une catégorie particulière de données protégées par l'art. 9 RGPD. En dépit de cette reconnaissance, la Chambre admet que la défenderesse n'était pas tenue, au moment des faits, de notifier ladite violation à l'autorité de contrôle.

Cette conclusion repose sur une lecture contextualisée des obligations de l'art. 33 RGPD. La Chambre rappelle que la notification constitue le principe, tandis que l'absence de notification ne peut s'envisager qu'à titre d'exception, dans les cas où il peut être démontré que la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés de la personne concernée. En l'espèce, elle constate que la défenderesse, après concertation entre son DPO et son service juridique, a estimé que l'atteinte ne présentait pas un tel risque substantiel. Elle note également que la plaignante a été personnellement informée de l'incident et que celui-ci est demeuré circonscrit à son dossier, sans diffusion ultérieure.

Néanmoins, la Chambre émet de sérieuses réserves sur l'analyse de risque effectuée par la défenderesse. Elle relève en particulier que le simple fait que des données de santé aient été consultées en dehors de toute finalité thérapeutique suffisait à caractériser un risque pour les droits de la personne concernée, notamment en termes de perte de confidentialité et de perte de contrôle sur des données couvertes par le secret professionnel. L'argument tenant au caractère isolé de la violation est également écarté, le RGPD ne subordonne pas l'existence d'un risque à la pluralité des personnes concernées. Dès lors que la nature des données est sensible et que les circonstances de l'accès sont anormales, le seuil de risque apparaît franchi.

La portée de cette critique est toutefois atténuée par la prise en compte, par la Chambre, du contexte temporel. Elle considère en effet que les faits se sont déroulés au début de l'année 2020, à une époque où les lignes directrices du Comité européen de la protection des données (CEPD) relatives à la notification des violations n'étaient pas encore adoptées. La Chambre souligne également que la maturité opérationnelle des responsables de traitement en matière de notification était encore en phase d'évolution, ce qui justifie une forme d'indulgence rétroactive. Ce raisonnement conduit à ne pas sanctionner l'absence de notification, tout en affirmant avec fermeté que, dans le contexte réglementaire actuel, une telle omission ne saurait plus être tolérée.

Ce traitement différencié, fondé sur l'évolution dans le temps des standards de conformité, traduit une approche pragmatique, mais il peut susciter une certaine perplexité quant à l'unité d'application du droit. Surtout, il pose la question de l'équilibre entre l'objectif pédagogique de la régulation et l'impératif de protection effective des personnes concernées, particulièrement dans des cas impliquant des données aussi sensibles que celles relatives à la santé. Ainsi, même si la décision reflète une volonté de proportionnalité dans l'appréciation des faits, elle contribue également à alimenter le débat sur la rigueur attendue des responsables de traitement face à des incidents de sécurité engageant la confidentialité des données médicales.

Conclusion

La décision 64/2025 de la Chambre Contentieuse s'inscrit dans une démarche d'équilibre entre rigueur juridique et pragmatisme institutionnel. Elle se distingue par une lecture nuancée des faits, soucieuse de replacer l'application du RGPD dans son contexte opérationnel, mais elle n'en soulève pas moins plusieurs interrogations de fond.

En affirmant que la supérieure hiérarchique ayant consulté le dossier médical de la plaignante agissait en qualité de responsable autonome du traitement, la Chambre adopte une interprétation restrictive de la notion d'autorité du responsable de traitement, qui tend à diluer la portée du principe d'« accountability ». Or, même en présence d'un comportement fautif isolé, il peut être soutenu que l'entité employeuse demeure tenue de garantir, par des mesures organisationnelles appropriées, la prévention et la détection des usages illicites de données personnelles sensibles.

Par ailleurs, la reconnaissance explicite d'un risque pour les droits et libertés de la personne concernée, combinée à la nature des données aurait logiquement dû conduire à une obligation de notification à l'autorité de contrôle. Le fait que la Chambre justifie l'absence de notification par le contexte réglementaire de l'année 2020 témoigne d'une volonté d'adapter l'appréciation des obligations au degré de maturité des pratiques en matière de sécurité de l'information. Cette tolérance, si elle se comprend du point de vue de la proportionnalité, pourrait néanmoins être perçue comme un précédent affaiblissant l'effectivité de l'art. 33 RGPD.

En somme, cette décision met en lumière les tensions inhérentes à l'application du RGPD, entre exigence de conformité et prise en compte des réalités du terrain, entre sanction et accompagnement. Elle offre une lecture contextualisée de la régulation, qui a le mérite d'être pédagogique, mais qui appelle également à une vigilance accrue pour garantir que les prin-

cipes de protection des données, notamment en matière de santé, ne soient pas affaiblis au nom de la flexibilité.

Proposition de citation : Anna Ploix, Dossier médical du salarié consulté par l'employeur : jusqu'où va la souplesse du RGPD ?, 3 juillet 2025 *in* www.swissprivacy.law/364