HERBERT SMITH FREEHILLS

PARIS E-BULLETIN

Novembre 2022

Comment concilier les demandes de droit d'accès aux données personnelles avec les intérêts de l'entreprise ?

Demandes de droit d'accès, secrets commerciaux et risques contentieux : bonnes pratiques et pièges à éviter.

- Les demandes de droit d'accès intervenant dans un contexte contentieux, notamment prud'homaux et civils, ont récemment connu une rapide augmentation.
- À la suite d'une réponse incomplète ou insatisfaisante, les auteurs de la demande de droit d'accès peuvent saisir la CNIL, qui est susceptible de prendre contact avec la société ou de procéder à un contrôle.
- La CNIL a reçu pour l'année 2021 plus de 300 plaintes liées à un mauvais traitement d'une demande d'exercice de droit par un salarié ou ancien salarié.

Comment appliquer la balance entre l'obligation de répondre à la demande de droit d'accès et la défense des intérêts de l'entreprise ou des tiers (protection du secret des affaires, du secret des correspondances…) ?

La présente fiche vise à fournir aux entreprises un guide de gestion des demandes de droit d'accès, accompagné des bonnes pratiques présentées par les intervenants à la conférence.

Etape 1 : Vérifier l'identité de la personne concernée

- Toute personne peut exercer son droit d'accès auprès d'une entreprise (salarié, utilisateur, client, prestataire...).
- **Bonne pratique** : l'entreprise peut s'assurer de l'identité de la personne sur la base d'indices. Exemple : pour un salarié, l'identité peut être vérifiée si la demande est réalisée depuis son adresse e-mail profesionnelle.
- Si un doute subsiste, l'entreprise pourra demander des éléments complémentaires d'identification (numéro d'identification, matricule, ou si aucun élément n'est pertinent, une copie d'une pièce d'identité).
- **Bonne pratique** : accuser réception de la demande de droit d'accès dès réception

Etape 2 : Identifier le champ de la demande

- La demande d'accès peut porter soit sur des données spécifiques (courriers électroniques professionnels, éléments relatifs aux heures supplémentaires, etc.) soit sur l'ensemble des données à caractère personnel concernant l'auteur de la demande.
- L'entreprise vérifie dans un premier temps si la demande présente un caractère infondé ou excessif, notamment si la demande est répétitive.
- L'entreprise effectue, dans un second temps, une recherche pour identifier les données entrant dans le champ de la demande et obtenir une estimation de leur volume. Pour effectuer cette recherche, la société pourra s'appuyer sur des mots clés pertinents.
- **Bonne pratique** : conserver une trace des mots-clés utilisés (par exemple, dans le registre de gestion des demandes d'exercices de droits) afin d'en justifier la pertinence en cas de demande par la CNIL.
- Sauf précision spécifique de l'auteur de la demande, la société doit effectuer la recherche sur l'ensemble des supports (informatique, papier...).
- **Bonne pratique** : un traitement attentif doit être accordé à une demande émanant d'un salarié. Un salarié a une connaissance approfondie du fonctionnement de la société et des traitements réalisés sur ses données à caractère personnel. Un salarié sera en général plus attentif à la réponse donnée par l'entreprise.

Etape 3 : Préciser le champ de la demande si nécessaire

- Sur la base des informations issues de l'extraction, l'entreprise pourra déterminer si la demande couvre un volume conséquent ou limité de données. Si la demande couvre un volume conséquent de données ou que les données sont difficiles à extraire, l'entreprise pourra augmenter le délai de réponse d'une durée de 2 mois (voir la section « Dans quel délai répondre à la demande ? »).
- **Bonne pratique** : lorsque la demande porte sur un nombre conséquent de données, la société peut inviter la personne concernée à préciser le champ de sa demande, par exemple, la nature des informations souhaitées, les supports de collecte des données pertinents.

L'entreprise pourra également lui soumettre une proposition de mots-clés pertinents afin d'affiner la recherche et y répondre de manière appropriée.

- Toutefois, la personne a le droit de confirmer le champ initial de sa demande ou de ne pas donner suite à cette demande de précision.

Etape 4 : Répondre à la demande de droit d'accès

- L'entreprise doit assurer la conciliation entre le droit de la personne concernée à recevoir une copie de ses données à caractère personnel et la protection des droits et libertés des tiers et d'elle-même.
- La demande ne doit pas permettre à la personne concernée de recevoir des informations sur un tiers (respect de la vie privée, secret des correspondances) ou qui porterait atteinte à un tiers ou à la société (telle qu'une information relevant du secret des affaires ou de sa propriété intellectuelle).
- **Bonne pratique** : une demande de droit d'accès donne droit à une copie des données personnelles et non aux documents contenant des données à caractère personnel. L'entreprise a le droit de communiquer un tableau énumérant la nature des documents concernés et les données figurant dans ceux-ci.
  Exemple : un courrier électronique concernant un projet commercial sensible qui comporterait uniquement le patronyme du salarié pourrait être mentionné en précisant que ce document est un compte-rendu commercialement sensible sur lequel figure le patronyme du salarié, mais qu'il n'est pas communiqué car il est relatif à une procédure interne ou à un projet commercial.
- La société peut procéder à une revue des documents identifiés et supprimer (par exemple par une méthode de caviardage) ou anonymiser le contenu afin de n'y faire figurer que les données à caractère personnel du salarié. Certains documents peuvent contenir des données à caractère personnel sans expressément mentionner le salarié (par exemple, un compte-rendu d'évaluation de performance peut contenir des informations personnelles sur le salarié).
- **Point d'information** : une demande de droit d'accès qui aurait des conséquences intrusives sur l'entreprise ou des tiers pourrait être considérée comme excessive. Le Conseil d'Etat instruit actuellement une demande de droit d'accès d'un salarié à l'ensemble des messages échangés et l'ensemble des informations le concernant, pour déterminer si celle-ci pouvait être excessive ou non au regard de l'absence de délimitation de sa demande.
- La réponse devra être transmise par le canal par lequel la personne a effectué sa demande, à moins que la personne concernée ne demande qu'il en soit autrement.

Quel délai pour répondre à une demande de droit d'accès ?

- Principe : un mois à compter de la réception de la demande.

- Exception : le délai peut être rallongé de deux mois supplémentaires lorsque la demande est complexe ou multiple. L'auteur de la demande doit systématiquement être informé de l'extension du délai de principe.
- Le rallongement du délai doit être justifié, par exemple parce que la demande est étendue en nature et dans le temps.
- **Bonne pratique** : conserver les preuves justifiant le rallongement du délai pour les présenter à la CNIL en cas de demande.
- A l'exception d'une volonté manifeste de l'entreprise de nuire à la personne concernée ou d'avoir méconnu la demande, la CNIL devrait accepter une demande de rallongement de délai.
- **Bonne pratique** : en cas de demande complexe ou étendue, l'entreprise peut répondre de manière séquencée en envoyant communication des données en plusieurs temps. Le séquencage doit toutefois être justifié par l'entreprise.

Quelle sanction en cas de d'absence de réponse ou de réponse incomplète à une demande de droit d'accès ?

- La CNIL peut être saisie d'une plainte par une personne qui ne serait pas satisfaite de la réponse apportée à sa demande de droit d'accès.
- La CNIL a une obligation de rendre compte à un plaignant des suites de sa demande et notamment des actions engagées auprès de l'entreprise.
- **Point d'information** : la CNIL réalise beaucoup de contrôles faisant suite à une mauvaise gestion d'une demande de droit d'accès.
- La CNIL ne prend pas en compte le fait qu'une demande de droit d'accès intervienne ou non dans un cadre contentieux.
- Cependant, elle peut prendre en compte la situation du plaignant qui souhaiterait obtenir une réponse dans le cadre d'une audience lorsque l'urgence le justifie, notamment en cas de risque de suppression des données.
  Exemple: images de vidéosurveillance qui font l'objet d'un délai de conservation court.
- Avant de procéder à un contrôle, la CNIL peut engager un échange avec l'entreprise sur les actions mises en place pour répondre à l'exercice du droit, et notamment de la méthodologie utilisée (le pourquoi et le comment de la gestion de la demande). La CNIL vérifie la pertinence de la réponse apportée et dans quelle mesure celle-ci a été satisfaite.
- En cas de contrôle, la CNIL ne se limite pas à la demande de droit d'accès et à la réponse apportée. Elle peut contrôler l'ensemble des traitements réalisés par l'entreprise. La CNIL contrôle notamment les durées de conservation des données, les mesures de sécurité mises en place ou la détermination d'une base légale adéquate qui sont les écarts les plus constatés en pratique.
- A l'issue du contrôle, la CNIL peut prononcer les sanctions suivantes :

    - Rappel à l'ordre,
    - Injonction de répondre à la demande sous astreinte,
    - Sanction financière pouvant aller jusque 20 000 000 euros ou 4% du chiffre d'affaires mondial de l'année précédente de la société.

- La CNIL a développé une procédure « *fast track* » pour le traitement des dossiers simples tels que les plaintes liées à l'exercice du droit d'accès. Dans le cadre de cette procédure simplifiée, la CNIL peut prononcer des amendes administratives d'un montant maximum de 20 000 euros et une injonction avec astreinte d'un montant maximum de 100 euros par jour.

Traitement des courriers électroniques professionnels d'un salarié

- La demande de droit d'accès peut amener la société à transmettre des données à caractère personnel issues de courriers électroniques transmis ou reçus par la personne concernée ou lorsque celle-ci est mentionnée par des tiers dans un échange.
- L'entreprise doit apporter un traitement différent aux courriers électroniques selon que l'auteur de la demande d'accès est destinataire ou expéditeur d'un courrier électronique ou bien si elle est simplement mentionnée dans un échange entre tiers.
- Situation 1 : l'auteur de la demande est destinataire ou expéditeur d'un courrier électronique. Dans ce cas, la personne a en principe connaissance des informations contenues dans ces courriers et peut légitimement en recevoir une copie (sous réserve des exceptions mentionnées dans la section « *Etape 4 : Répondre à la demande de droit d'accès »*). Le salarié en poste peut accéder à sa boite de messagerie. Néanmoins en cas de demande la communication pourrait être limitée aux courriers électroniques qu'il indique ne plus avoir en sa possession.
- Situation 2 : la personne concernée est simplement mentionnée dans un échange entre tiers. Dans ce cas, l'entreprise doit s'assurer que la communication des courriers électroniques ou des données personnelles issues de celui-ci ne portent pas atteinte à l'entreprise ou à un tiers. Le cas échéant, l'entreprise pourra refuser de les communiquer en justifiant d'un risque pour les droits des tiers ou de l'entreprise auprès de l'auteur de la demande. L'entreprise devra être attentive à supprimer ou anonymiser toute information ne concernant pas le demandeur.