La gestion des habilitations et des accès informatiques

Afin de sécuriser les systèmes d'information (SI) et de garantir la confidentialité des données que celui-ci contient, la mise en place de système d'habilitations est aujourd'hui de plus en répandu sur le lieu de travail. Ce système permet en effet de s'assurer que **chaque** utilisateur du SI ne puisse accéder qu'aux données dont il a besoin pour l'exercice de sa mission, ce qui se traduit au niveau interne par la mise en place d'un mécanisme de définition des niveaux d'habilitation d'un utilisateur dans le système, et d'un moyen de contrôle des permissions d'accès aux données.

Qu'est-ce qu'une habilitation ?

L'habilitation est fonction d'un profil préalablement défini, généralement lié à une **position hiérarchique** ou à une **fonction** au sein de la structure, et non à une personne déterminée.

Cela permet de faciliter la gestion des accès en cas de mouvement de personnel. Au contraire, lorsque les accès sont attribués par personne, il convient d'être extrêmement réactif et de supprimer sans délai tout accès en cas de départ d'un membre du personnel du service ou de la structure.

L'habilitation doit conférer ainsi à chaque utilisateur les droits qui sont **strictement nécessaires à l'accomplissement de ses attributions**. A ce titre, elle doit déterminer, notamment :

- les données et applications auxquelles celui-ci peut avoir accès, de manière dédiée ou partagée (réseau local ou partagé, dossiers de travail, imprimantes, téléphones, etc.) ;
- l'étendue des droits ainsi conférés : accès en simple consultation, en inscription, en suppression.

Dans quels buts un employeur peut-il mettre en place un système d'habilitations ?

Les données personnelles peuvent être collectées pour **plusieurs finalités**, à condition que ces finalités soient :

- **déterminées** ;
- **explicites** ;
- **légitimes** ; et
- **non traitées ultérieurement de manière incompatible** avec ces finalités.

En vertu de ce principe de **limitation des finalités**, l'APDP considère que la mise en place d'un dispositif de gestion des habilitations peut répondre aux objectifs suivants :

Dans le cadre de la gestion des habilitations *:*

- octroyer / délivrer aux utilisateurs du SI les moyens techniques et fonctionnels permettant de s'authentifier au système d'information afin de pouvoir exercer la fonction et les missions pour lesquelles ils ont été recrutés ;
- gérer les évolutions de droits, les mobilités internes et les départs ;
- mettre à jour les comptes systèmes dans le cadre de changement d'informations administratives (ex : changement de patronyme) ;
- permettre la réalisation de l'ensemble des tâches d'activation/ désactivation/suppression de comptes ;
- procéder à des revues de contrôles périodiques afin de s'assurer de la conformité des droits délivrés par rapport aux demandes et aux règles édictées en matière d'accès à l'information.

Dans le cadre de la supervision des accès aux applications :

- collecter des évènements systèmes (logs) permettant de tracer les accès des utilisateurs aux applications et données ;
- établir des alertes et/ou des rapports qui permettent de détecter tout risque de malveillance et de s'assurer de la cohérence des accès avec les habilitations délivrées ;
- établir des preuves en cas de litige avec tout utilisateur (employé, prestataire…).

Dans le cadre de la sécurité anti-virus :

- mettre en place des remontées d'alertes sur les risques d'intrusion ;
- établir des rapports (ex : audit de sécurité, détection de risques…).

Quid de la notion de surveillance ou de contrôle
Un employeur peut décider de procéder au contrôle ou à la surveillance des habilitations informatique mises en place au sein de son entité. A cet égard, l'APDP considère que cette notion de contrôle ou de surveillance du système de gestion des habilitations se conçoit comme « *toute activité qui consiste en la collecte, la détection et/ou l'enregistrement, dans le cadre de rapports établis à intervalles réguliers, des données à caractère personnel d'une ou de plusieurs personnes, relatives à l'utilisation des habilitations informatiques* ».

Quelle justification pour la mise en place d'un système de gestion des habilitations ?

Pour être licite, un traitement automatisé de données personnelles doit répondre à au moins une des exigences prévues à l'article 5 de la Loi n° 1.565 du 3 décembre 2024.

L'APDP estime ainsi que la mise en place d'un système de gestion des habilitations peut être justifiée par :

- ***Le respect des obligations légales du responsable du traitement***

Certains responsables du traitement sont soumis à des obligations particulières de **vigilance** ainsi que de **traçabilité des opérations effectuées**. Ainsi, pour les établissements bancaires ou assimilés, de telles obligations sont prévues, entre autres, par les textes suivants :

- la Loi n° 1.338 du 7 septembre 2007 sur les activités financières et son Ordonnance Souveraine d'application ;
- la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, et son Ordonnance Souveraine d'application ;
- la Loi n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financiers ;
- l'Arrêté Ministériel n° 2012-199 du 5 avril 2012 relatif aux obligations professionnelles des établissements de crédit teneurs de comptes-conservateurs d'instruments financiers.

L'APDP estime qu'afin de respecter leurs obligations, ces responsables du traitement ou leurs représentants peuvent mettre en place des procédures de surveillance ou de contrôle des habilitations informatiques, dans le strict respect toutefois des principes définis par la Loi n° 1.565 du 3 décembre 2024, notamment les principes de **proportionnalité** et de **transparence**.

➢ ***La réalisation d'un intérêt légitime poursuivi par le responsable de traitement ou un tiers***

L'APDP considère qu'une procédure de surveillance ou de contrôle des habilitations informatiques peut également être justifiée par un **intérêt légitime** du responsable du traitement ou un tiers, tel que :

- l'optimisation de l'accomplissement des missions de travail de ses employés ;
- la sécurité et le bon fonctionnement technique du réseau ou système informatique ;
- la préservation des intérêts économiques, commerciaux ou financiers du responsable du traitement ou de son représentant ;
- la prévention et la détection a priori et a posteriori de toute activité non-conforme ou illicite, par des utilisateurs.

Eu égard à l'existence d'un **lien de subordination** ou d'un **lien contractuel** entre l'employeur et l'employé, le consentement de ce dernier ne peut constituer une justification à la mise en œuvre de ce type de traitement.

Quels sont les grands principes en matière d'habilitations informatiques ?

➢ ***Des profils d'habilitation définis, formalisés et auditables***

En premier lieu, l'APDP rappelle qu'il est nécessaire pour toutes les catégories de comptes (nominatifs ou collectifs), d'identifier et d'authentifier tout utilisateur en fonction notamment du niveau de risque associé à la ressource, du type d'utilisateur ou encore du type d'accès. Cette séparation des tâches et des domaines de responsabilité permet ainsi de limiter l'accès à des données à caractère personnel aux seuls utilisateurs dûment habilités.

A cet égard, elle demande de respecter d'une part le principe du « besoin *d'en connaître* » qui correspond à la définition, par le métier, des habilitations nécessaires pour l'activité d'un utilisateur donné, et d'autre part le principe « *du moindre privilège* » qui consiste à mettre en place les habilitations strictement nécessaires aux activités liées à chaque compte.

L'APDP demande également que les modalités d'octroi des habilitations soient documentées.

Elle rappelle, par ailleurs, que les permissions d'accès des utilisateurs doivent être supprimées ou modifiées dès lors que ces derniers ne sont plus habilités à accéder à une ressource car ils ont quitté l'entité ou bien changé de fonctions.

L'APDP relève enfin qu'il est impératif de s'assurer du respect des règles de gestion des habilitations. Les propriétaires du système d'information doivent ainsi contrôler régulièrement la pertinence des profils et des accès accordés.

- ***Une politique de validation des habilitations et de gestion des mobilités***

L'APDP insiste sur le fait que toute demande d'habilitation doit être validée au moins par le responsable hiérarchique de la personne habilitée. Par ailleurs, si ledit responsable délègue cette tâche, il doit toutefois nécessairement conserver la responsabilité des habilitations de son équipe et de celles attribuées aux personnes effectuant des prestations de service pour son compte.

L'APDP demande également au responsable du traitement de veiller à la gestion efficace de tout changement de poste ou de départ afin d'éviter l'accumulation des habilitations. Ainsi lorsqu'une personne est mutée ou quitte l'entité, les habilitations dont elle disposait doivent être modifiées ou retirées immédiatement.

Quelles informations peuvent être collectées ?

Conformément aux dispositions de l'article 4 de la Loi n° 1.565 du 3 décembre 2024, les données à caractère personnel collectées doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles sont traitées* ».

L'APDP considère ainsi que seules les données personnelles suivantes peuvent être collectées et traitées :

- identité : nom, prénom et service de l'employé, nom, prénom et signature du supérieur pour la gestion des habilitations ;
- données d'identification électronique : identifiants de la personne habilitée (login et mot de passe) ;
- compte utilisateur : nom du compte, domaine du compte, groupe d'utilisateurs, type de droits ;
- données de connexion : logs, traces d'exécution, horodatage, fichiers journaux.

Combien de temps peuvent être conservées les données collectées et traitées dans le cadre d'un système de gestion des habilitations ?

Les données personnelles collectées **ne peuvent être conservées indéfiniment** sous une forme permettant l'identification des personnes concernées.

Ainsi, l'APDP demande à l'employeur de prévoir les durées de conservation de données suivantes :

- s'agissant de l'identité et du compte utilisateur : 3 mois maximum après le départ de l'employé ;

- s'agissant des données d'identification électronique : la durée d'utilisation du S.I. par la personne concernée ;

- s'agissant des données de connexion : 1 an maximum à compter de leur collecte, en fonction de l'activité exercée.

En tout état de cause, l'APDP recommande, lorsque cela est possible, d'adopter une durée de conservation moindre, dès lors que les données traitées ne sont plus nécessaires à la réalisation de la finalité pour laquelle elles ont été initialement collectées.

Enfin, elle rappelle que dans le cadre de l'ouverture d'une procédure contentieuse, toute information nécessaire issue du traitement pourra être conservée jusqu'à la fin de ladite procédure.

Qui peut avoir accès aux données relatives aux habilitations ?

L'accès aux données relatives aux habilitations doit être limité aux **seules personnes** qui, dans le cadre de leur(s) fonction(s), peuvent **légitimement en avoir connaissance au regard des objectifs du dispositif**.

Ainsi, le service informatique peut par exemple avoir accès aux habilitations à des fins de création, modification et suppression des utilisateurs et des groupes de profils et le responsable LAB peut y accéder pour vérifier les niveaux d'habilitation des personnes en charge des traitements relatifs à la lutte contre le blanchiment de capitaux.

De même, un prestataire informatique peut également avoir tous les droits à des fins de maintenance. Ces droits d'accès doivent alors être limités à ce qui est **strictement nécessaire à l'exécution de son contrat de prestation de service**. De plus, ledit prestataire est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable du traitement.

L'APDP estime par ailleurs que la communication des données à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, ladite Direction ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées.

Enfin, l'APDP considère que l'Autorité Monégasque de Sécurité Financière (AMSF) et la Commission de Contrôle des Activités Financières (CCAF) peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires de données personnelles traitées.

Comment informer les personnes concernées ?

Tout employeur doit impérativement responsabiliser les utilisateurs à la protection de leurs données personnelles.

Dans un souci de **transparence** envers les utilisateurs, ainsi que de **loyauté** dans la collecte et le traitement des données personnelles, l'APDP recommande donc à l'employeur de mettre en place une charte d'usage des outils de communication électronique, venant préciser, notamment lorsque des procédures de contrôle ou de surveillance sont mises en œuvre :

- la ou les finalités de ces procédures ;
- les personnes habilitées à avoir accès au traitement ;
- la durée de conservation des données collectées ;
- les modalités d'exercice par les personnes de leurs droits d'accès à leurs données.

Enfin, l'APDP insiste sur la nécessité de mettre en œuvre une sensibilisation de l'ensemble des utilisateurs du SI non seulement sur les habilitations qui leurs sont accordées et des responsabilités qui en découlent, mais également sur le fait que toutes leurs actions sont tracées.

Quelle sécurité mettre en place ?

L'APDP rappelle que les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du traitement.

Elle préconise que l'authentification soit effectuée par un **identifiant** et un **mot de passe individuel réputé fort régulièrement changé**.

Par ailleurs, les accès des personnes habilitées devront faire l'objet d'une **journalisation.**

L'APDP demande en outre à ce que les personnes habilitées à avoir accès au traitement soient astreintes à une **obligation de confidentialité particulièrement stricte**, précisée par écrit (par exemple dans une charte informatique, une charte administrateur ou le contrat de travail).

Enfin, elle admet que des données puissent être extraites et/ou copiées sur un support distinct en vue d'une communication aux Autorités administratives ou judiciaires légalement habilitées. Elle rappelle que dans ce cas, toute copie ou extraction de ces données devra être **chiffrée sur son support de réception**.