Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Le préposé fédéral à la protection des données et à la transparence**
**PFPDT**

Version 1.0

# Recommandations techniques du PFPDT relative à la journalisation prévue à l'art. 4 OPDo

15 septembre 2023

# Table des matières

# 1. Introduction et objectif du document

Depuis l'entrée en vigueur de l'art. 4 de l'ordonnance sur la protection des données (OPDo)[1], le 1er septembre 2023[2], le responsable du traitement privé et son sous-traitant privé doivent au moins journaliser l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données lors du traitement automatisé de données personnelles.

Les présentes recommandations visent à fournir un aperçu de ce qu'implique la journalisation et les exigences techniques à remplir pour satisfaire à l'art. 4 OPDo. La mise en œuvre concrète sera définie par les propriétaires de systèmes et ne fait pas partie des présentes recommandations. Outre l'OPDo, d'autres directives de la Confédération peuvent s'appliquer, notamment celles relatives à la sécurité de l'information. L'objectif est de parvenir à une journalisation aussi efficace que possible, en évitant les doublons.

## 1.1. Art. 4 OPDo

L'art. 4 OPDo relatif à la journalisation est formulé comme suit :

> [1] Lors de traitements automatisés de données sensibles à grande échelle ou de profilage à risque élevé et lorsque les mesures préventives ne suffisent pas à garantir la protection des données, le responsable du traitement privé et son sous-traitant privé journalisent au moins l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données. La journalisation est notamment nécessaire lorsque, sans cette mesure, il n'est pas possible de vérifier a posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées.
>
> [2] Lors du traitement automatisé de données personnelles, l'organe fédéral responsable et son sous-traitant journalisent au moins l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données.
>
> [3] Pour les données personnelles généralement accessibles au public, l'enregistrement, la modification, l'effacement et la destruction des données doivent au moins être journalisés.
>
> [4] La journalisation doit fournir des informations sur l'identité de la personne qui a effectué le traitement, la nature, la date et l'heure du traitement et, le cas échéant, l'identité du destinataire des données.
>
> [5] Les procès-verbaux de journalisation sont conservés durant au moins un an, séparément du système dans lequel les données personnelles sont traitées. Ils sont accessibles uniquement aux organes et aux personnes chargés de vérifier l'application des dispositions relatives à la protection des données personnelles ou de préserver ou restaurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, et ne peuvent être utilisés qu'à cette fin.

## 1.2. Art. 3, al. 3, OPDo

La journalisation permet d'assurer la traçabilité du traitement des données personnelles et en particulier de l'accès à celles-ci. Cet objectif est énoncé à l'art. 3, al. 3, OPDo, qui décrit ce que la journalisation doit permettre d'accomplir :

> [3] Pour assurer la traçabilité, le responsable du traitement et le sous-traitant prennent des mesures appropriées afin que :
>
> a. il soit possible de vérifier quelles données personnelles sont saisies ou modifiées dans le système de traitement automatisé de données, par quelle personne et à quel moment (contrôle de la saisie);
>
> b. il soit possible de vérifier à qui sont communiquées les données personnelles à l'aide d'installations de transmission (contrôle de la communication);

[1] Ordonnance du 31 août 2022 sur la protection des données (OPDo, RS 235.11) (admin.ch)

c. les violations de la sécurité des données puissent être rapidement détectées (détection) et que des mesures puissent être prises pour atténuer ou éliminer les conséquences (réparation).

La traçabilité est aussi liée à la lecture des données. Cet aspect est couvert par l'enregistrement des accès en vue de détecter une violation du contrôle des accès, comme énoncé à l'al. 3, let. c.

## 1.3. But de la journalisation

Le but de la journalisation est de permettre la vérification a posteriori du traitement des données personnelles, de sorte à pouvoir établir ultérieurement si une personne ou une machine a accédé aux données ou si celles-ci ont été effacées, détruites ou modifiées. Il s'agit aussi de garantir que les données sont utilisées aux fins prévues et suffisamment protégées. Elle sert en outre à déceler et à faire la lumière sur les violations de la sécurité des données. La journalisation peut ainsi également aider à établir si des données personnelles n'ont pas été traitées conformément aux finalités prévues, à détecter des violations de la sécurité et à en déterminer les causes. En revanche, elle ne doit pas servir à surveiller le comportement des utilisateurs qui traitent des données personnelles.

# 2. Journalisation

Dans la législation sur la protection des données, la journalisation désigne l'enregistrement systématique d'informations sur le traitement des données personnelles. Elle a pour but de garantir la transparence et de satisfaire à l'obligation de rendre compte ainsi que, en cas de violation de la protection des données ou d'incident, de permettre d'identifier les personnes qui ont accédé à des données personnelles, et de déterminer ce qu'elles ont modifié et à quel moment.

## 2.1. Les trois piliers de la journalisation

La journalisation repose sur trois piliers : la saisie, l'enregistrement et l'analyse des données de journalisation.

Le responsable du traitement privé et son sous-traitant privé doivent au moins journaliser l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données. La journalisation est notamment nécessaire lorsque, sans cette mesure, il n'est pas possible de vérifier a posteriori que les données ont été traitées aux fins pour lesquelles elles ont été collectées ou communiquées.

Le processus de « lecture » doit être compris comme un accès sans « modification »; il suffit par conséquent de journaliser les accès aux données personnelles et les modifications de celles-ci pour satisfaire aux exigences de journalisation relatives à la « lecture ». Il convient de mentionner ici la restriction prévue à l'art. 4, al. 3, OPDo pour les données personnelles généralement accessibles au public. L'enregistrement, la modification, l'effacement et la destruction de ces données au moins doivent être journalisés.

### 2.1.1. Saisie

Les données de journalisation doivent être saisies afin de garantir l'enregistrement de toutes les opérations concernant les données personnelles. Cela signifie que tous les accès (par des personnes ou des machines) à des données personnelles doivent être journalisés, y compris l'identité de la personne qui a effectué le traitement, la nature, la date et l'heure du traitement et, le cas échéant, l'identité du destinataire des données.

### 2.1.2. Enregistrement

Les données de journalisation doivent être stockées de manière sécurisée et protégée, séparément des systèmes de traitement des données afin de garantir leur disponibilité même

si le système principal est en dérangement (p. ex. à la suite d'une attaque par un rançongiciel). L'accès doit être limité aux personnes autorisées auxquelles il incombe de vérifier l'application des dispositions relatives à la protection des données ou de préserver ou restaurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données.

#### 2.1.3. Analyse

Les données de journalisation doivent pouvoir être analysées en cas de besoin afin de détecter d'éventuelles violations de la protection des données et de garantir que tous les accès aux données personnelles sont conformes à la loi. Cela nécessite des outils d'analyse puissants, capables de traiter de grandes quantités de données de journalisation et d'identifier des modèles ou des anomalies qui pourraient indiquer des violations. Les données de journalisation doivent être accessibles uniquement aux organes et aux personnes chargés de vérifier l'application des dispositions relatives à la protection des données personnelles ou de préserver ou restaurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, et ne peuvent être utilisées qu'à cette fin (art. 4, al. 5, OPDo).

### 2.2. Plan

Un plan de journalisation doit être élaboré ou repris. Il doit comprendre une description complète et systématique de la politique et des procédures en matière de journalisation ainsi que les éléments principaux suivants :

a) Buts de la journalisation : le plan doit définir des objectifs clairs que la journalisation doit permettre d'atteindre, p. ex. la surveillance du traitement des données personnelles, la surveillance de la sécurité, l'élimination des erreurs.

b) Lignes directrices en matière de journalisation : le plan doit fixer des lignes directrices claires pour la journalisation, soit préciser notamment les incidents à journaliser, les données à saisir, la durée de conservation prévue et les personnes autorisées à accéder aux données de journalisation.

c) Outils de journalisation : le plan doit indiquer les outils utilisés pour la journalisation, par exemple les agents de journalisation, les outils de gestion des procès-verbaux de journalisation, l'infrastructure de journalisation des événements ou les systèmes de gestion des informations et des événements de sécurité (security information and event management, SIEM).

d) Plan d'alerte : le plan doit préciser les événements susceptibles de déclencher une alerte, comment réagir à ces alertes, les personnes devant être informées et les mesures devant être prises en cas de détection de problèmes.

e) Responsabilités et rôles : le plan doit définir des responsabilités et des rôles clairs pour l'administration de la journalisation, par exemple qui est responsable de la surveillance de la journalisation, qui octroie les droits y relatifs et qui met à jour les lignes directrices en matière de journalisation. Il doit en outre préciser qui est responsable de l'analyse et de l'établissement des rapports.

f) Formation : le plan doit décrire comment les collaborateurs chargés de la journalisation peuvent acquérir les connaissances et les compétences nécessaires pour travailler efficacement et en toute sécurité.

g) Vérification : le plan doit prévoir des révisions régulières de la politique et des procédures en matière de journalisation afin de garantir leur efficacité et leur conformité aux exigences actuelles.

Il est essentiel de disposer d'un plan détaillé pour contrôler l'adéquation et la proportionnalité de la politique en matière de journalisation ainsi que le respect des exigences relatives à l'accès légal aux données de journalisation.

# 3. Recommandations techniques

## 3.1. Recommandations techniques générales relatives à la journalisation

Il existe nombre de recommandations techniques relatives à la journalisation dans le domaine de la sécurité de l'information et de la protection des données. En voici les principales :

a) Utilisation de formats de journalisation standard : les formats de journalisation standard, tels que Syslog ou Common Event Format (CEF), permettent une journalisation uniforme des événements.

b) Lecture et interprétation des procès-verbaux de journalisation : en plus d'être classés, les procès-verbaux de journalisation sont aussi lus et interprétés (parsing et indexing) à des fins de surveillance, de diffusion d'alertes et de détection d'anomalies. Il s'agit d'extraire tous les éléments d'information par extraction de modèles lors de la lecture (ingestion), et de les compléter, lorsque c'est utile, par des informations provenant de procès-verbaux de journalisation existants (corrélation). Il convient, dans ce processus, d'omettre les champs d'information non utilisés afin, notamment, d'économiser de la mémoire.

c) Vérification régulière des données de journalisation : il convient de vérifier régulièrement que les données de journalisation sont complètes, qu'elles n'ont pas été manipulées et que les directives de sécurité sont respectées.

d) Mécanismes de détection d'anomalies : il convient de mettre en place des mécanismes de détection des anomalies dans les données de journalisation (p. ex. accès à partir de géolocalisations inhabituelles) afin de détecter les activités suspectes. Cela exige de définir au préalable les comportements normaux pour que les écarts puissent être constatés.

e) Mise en œuvre de mesures de sécurité pour les données de journalisation : il importe de mettre en place des contrôles d'accès appropriés pour les données de journalisation afin de les protéger contre les accès non autorisés.

f) Horodatage : les données de journalisation sont horodatées afin de consigner le moment précis de la survenue d'un événement dans le système. L'horodatage facilite la compréhension des liens chronologiques entre différents événements dans le système.

g) Synchronisation : la précision de l'horodatage dépend directement de la synchronisation précise de tous les systèmes du réseau. La synchronisation des horloges de tous les systèmes effectuée au moyen d'un serveur NTP commun permet de garantir la précision et la cohérence des données du journal.

h) Enrichissement de données : l'enrichissement de données consiste à compléter les données de journalisation par des informations supplémentaires afin de mieux comprendre les événements. Il peut s'agir par exemple d'informations de géolocalisation ou relatives au contexte de l'utilisateur, ou encore de données de configuration du système. Il en résulte une analyse plus précise et une identification plus rapide des atteintes potentielles à la sécurité. Du point de vue de l'enrichissement de données, il est important de ne saisir que des informations appropriées et nécessaires à la réalisation concrète de l'objectif, en l'occurrence de la journalisation. En cas de combinaison avec d'autres données ou de création de profils à l'aide de l'enrichissement des données, il faut faire appel au conseiller à la protection des données, si un tel conseiller existe pour votre unité administrative. Si un sous-traitant

est chargé de l'enrichissement des données, il faut en outre s'assurer que le mandant et le sous-traitant sont liés par un contrat en bonne et due forme répondant aux exigences fixées dans la LPD.

i) Alerte : les applications d'analyse des procès-verbaux de journalisation utilisées doivent pouvoir informer immédiatement les responsables lorsqu'elles détectent des anomalies ou des événements touchant à la sécurité.

En suivant ces recommandations techniques, les responsables de traitement privés peuvent assurer une journalisation complète, qui leur permet de surveiller et d'analyser les événements touchant à la sécurité, et de réagir efficacement.

## 3.2. Stockage et capacité de stockage

L'une des difficultés du traitement des données de journalisation a trait à la capacité de stockage requise. Les données doivent rester directement accessibles aux outils d'analyse aussi longtemps qu'elles peuvent servir à identifier et à réagir aux violations de la protection des données ou aux incidents touchant à la sécurité. Ce délai peut varier en fonction du type et de la taille de l'organisation, mais il s'étend généralement sur une période allant de quelques jours à plusieurs semaines. Durant cette période, les données peuvent être utilisées activement pour détecter des activités suspectes et réagir.

Une fois que les données de journalisation ne servent plus directement à l'analyse, mais restent utiles par exemple pour le contrôle du respect des dispositions relatives à la protection des données, il est possible de les déplacer dans un système de stockage à long terme. On peut ainsi les copier et les stocker dans un emplacement moins coûteux. Cela n'autorise évidemment pas à conserver les données plus longtemps que ce que prévoient les dispositions légales applicables. Les recommandations en la matière sont les suivantes :

a) Utilisation de supports de données appropriés : il convient d'utiliser pour le stockage à long terme des données de journalisation des supports appropriés qui ont une longue durée de vie et sont fiables.

b) Durée de conservation : il importe de définir une durée de conservation claire pour les données de journalisation afin d'éviter de les conserver inutilement. Il convient évidemment de respecter les exigences légales en matière de durée de conservation. La durée de conservation des données de journalisation en rapport avec le traitement de données personnelles est fixée à au moins un an.

c) Calculer le volume de stockage : pour calculer le volume de stockage nécessaire pour les données de journalisation, il faut tenir compte de différents facteurs, tels que la quantité de données générées, le nombre de systèmes sur le réseau et la durée de stockage. Afin d'éviter toute interruption du processus de journalisation, il est important de prévoir une capacité de stockage suffisante. Pour une planification des capacités de stockage et une estimation des coûts optimales, il faut partir du principe que les données seront conservées pendant une ou deux semaines dans l'index puis stockées pendant au moins un an dans le système de stockage à long terme.

En résumé, le stockage à long terme des données de journalisation fait partie de la stratégie de sauvegarde des données. Il est important que les données de journalisation soient conservées séparément du système dans lequel les données personnelles sont traitées (conformément à l'art. 4 OPDo) afin de garantir leur intégrité et leur disponibilité. Il n'est normalement pas nécessaire de créer une copie de sauvegarde supplémentaire des données de journalisation sur un autre système, à condition de disposer d'une solution de stockage robuste et de contrôler régulièrement que les données soient complètes. Il convient toutefois de décider au cas par cas si une copie de sauvegarde des données de journalisation est nécessaire.

## 3.3. Journalisation pour les applications existantes

Avec des nouvelles applications, il est relativement facile de journaliser toutes les activités de traitement de données personnelles dès le début. En revanche, il n'est pas toujours possible de modifier les applications existantes, plus anciennes. Il existe cependant différentes solutions pour ces cas de figure.

La mise en œuvre de la journalisation dépend de nombreux critères, comme le langage de programmation, l'environnement d'exécution et les méthodes de développement utilisées pour l'application. Les recommandations ci-après revêtent par conséquent un caractère générique, mais elles peuvent être utiles pour la planification du processus dans les cas concrets.

**1re étape : connaître les exigences de la journalisation pour l'application**

Il faut déterminer la durée d'indexage et de conservation des procès-verbaux de journalisation dans l'espace de stockage à long terme. La durée de conservation (prescrite par la loi) a une incidence sur le calcul de la capacité de stockage et du volume des données (5e étape).

**2e étape : connaître les opérations de traitement devant être journalisées**

Toutes les activités d'une application ne constituent pas un traitement de données personnelles devant être journalisé. Il est utile d'établir une liste des activités à journaliser afin de focaliser le travail sur ces activités. Le but de la journalisation est de saisir les activités énoncées dans l'OPDo, et non pas d'enregistrer le plus grand nombre possible d'activités.

Avec certaines applications qui traitent des données personnelles, il n'est pas toujours possible de connaître la nature précise de ces traitements (p. ex. dans un système de documentation). Dans ce cas, il faut journaliser toutes les activités.

Pour renforcer la sécurité de l'information de l'application, il peut être souhaitable de journaliser également les événements critiques en matière de sécurité.

**3e étape : connaître les flux d'informations qui déclenchent des activités de traitement**

Il existe différents types d'applications :

- Dans la plupart des cas, le traitement de données personnelles déclenche une communication (c'est-à-dire un flux d'informations) entre le niveau de présentation (front end) et la logique administrative (back end). Ces flux d'informations traversent souvent plusieurs réseaux et systèmes de sécurité (voir figure 1), qui enregistrent au moins une partie des activités et peuvent par conséquent être utiles pour la journalisation, notamment en ce qui concerne la sécurité de l'information.

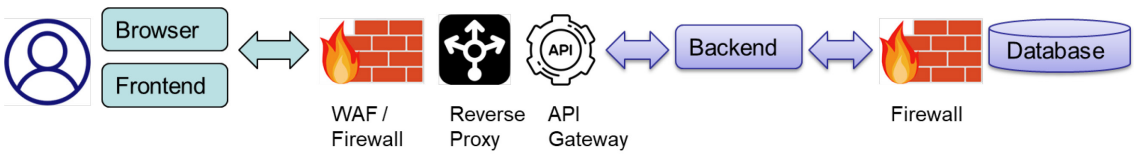


*Figure 11- Exemple de flux d'informations dans l'application*

- Si le traitement se limite au niveau de l'utilisateur et n'entraîne aucune communication avec des back ends sur un serveur ou avec des banques de données, le premier téléchargement sur le système de l'utilisateur doit être journalisé en tant qu'« accès ». Dans ce cas, généralement seule une extension de l'application permettrait d'enregistrer les modifications, ce qui ne serait utile que dans des cas exceptionnels.
- Avec certaines applications, le traitement est effectué de manière autonome par un processus dans le back end (p. ex. l'appariement automatisé de différentes données personnelles à des profils, l'extension automatisée de données personnelles telles que

les identifiants des utilisateurs avec les noms correspondants, etc.). Ici aussi, une extension de l'application sera souvent nécessaire.

**4e étape : décider où la journalisation peut et doit être mise en place**

Après avoir identifié les activités devant faire l'objet d'une journalisation et les flux d'informations, il convient d'évaluer la manière la plus simple d'intégrer la journalisation. Le NCSC recommande la procédure suivante :

1. La plupart des applications prennent en charge une journalisation des activités, mais elle est en général désactivée et doit être activée. Il convient par conséquent de vérifier ce point en premier. Si les applications comportent déjà une fonction de journalisation qui couvre toutes les activités et inclut suffisamment d'informations (c'est-à-dire l'identité de la personne qui reçoit ou traite les données personnelles, ainsi que la nature du traitement), la solution est simple.
2. Certains systèmes de réseau fournissent déjà suffisamment d'informations sur les activités (p. ex. l'identifiant des de l'utilisateur à partir de l'adresse IP et l'activité en lien avec le back end). Si c'est le cas, les procès-verbaux de journalisation du pare-feu ou du *Web Application Firewall* (WAF) peuvent déjà suffire à répondre aux exigences.
3. Un serveur Internet ou un proxy inverse peut souvent voir les requêtes décryptées. Ces systèmes prennent également en charge la journalisation d'activités. Ils peuvent saisir des requêtes de communication de manière sélective et les transmettre à un système d'analyse de procès-verbaux de journalisation.
4. Les applications modernes comportent également des passerelles API qui centralisent toutes les requêtes de l'utilisateur au back end ou entre les back ends (en cas de traitement automatisé) et les transmettent au back end concerné. Ces passerelles voient le contenu des requêtes. Il est possible d'y ajouter une journalisation sans qu'il soit nécessaire de modifier l'application.
5. La lecture et la modification de données personnelles se font généralement par le biais de systèmes de base de données, qui incluent presque toujours une journalisation des requêtes correspondantes.
6. Si aucune des recommandations précédentes ne peut être mise en œuvre, une extension de l'application sera nécessaire. Il est également possible de créer un wrapper. Cette application supplémentaire permet d'éviter de modifier l'application de base : elle centralise toutes les requêtes, les journalise et les transmet à l'application à proprement parler, sans procéder à aucune autre modification.

**5e étape : calculer la capacité de stockage et les systèmes d'analyse**

Les décisions prises dans les étapes précédentes permettent de calculer la capacité de stockage requise (voir ch. 3.3) et de définir avec le fournisseur de prestations du système récepteur les détails de la lecture et de la surveillance des procès-verbaux de journalisation.

## 4. Questions concrètes sur la mise en œuvre / FAQ

Les questions pratiques suivantes ont été soumises au NCSC. La liste sera complétée au fur et à mesure.

1) *Faut-il appliquer toutes les recommandations énoncées dans ce document ?*

Les présentes recommandations concernant la journalisation sont de nature générale. La journalisation est nécessaire pour garantir la cybersécurité des systèmes et une certaine traçabilité après des incidents. L'art. 4 OPDo ne prescrit pas l'utilisation d'un outil d'analyse, et nous partons du principe que de nombreux systèmes de traitement des données sont par défaut en mesure d'effectuer la journalisation supplémentaire exigée. L'ordonnance oblige uniquement à copier et à déplacer les données de journalisation. Leur conservation et leur analyse en ligne ne sont pas obligatoires dans le seul objectif de la protection des données. En revanche, elles le sont dans le cadre de la cybersécurité.

2) *Que signifie « généralement accessibles au public » ? Comment déterminer de manière fiable si les données sont généralement accessibles au public ?*

Les données sont « généralement accessibles au public » si leur accès ne requiert pas d'authentification, par exemple celles qui sont disponibles sur un serveur web. Sont également qualifiées de « généralement accessibles au public » les informations qui sont largement accessibles, comme les résultats d'une recherche d'adresse effectuée sur un site internet. L'art. 4, al. 3, OPDo prévoit une exception pour ces données : seuls l'enregistrement, la modification, l'effacement et la destruction doivent être journalisés. Le but de cette disposition est d'établir que la journalisation de la lecture et de la communication de ces données personnelles n'est pas obligatoire.

3) *Quel est le niveau de confiance autorisé pour la détermination de l'identité (conformément au ch. 4) pour la journalisation (identifiant Google, Facebook ou 2FA) ?*

La journalisation porte sur l'identité des personnes chargées du traitement des données. Elle ne dépend par conséquent pas du niveau de confiance (level of assurance).

4) *Que se passe-t-il si les systèmes actuels ne peuvent pas satisfaire à ces exigences et ne le pourront pas non plus à l'avenir ?*

Pratiquement tous les systèmes connus peuvent journaliser des données, sous une forme ou une autre. Si ce n'est pas le cas, il existe des applications tierces qui le font. Dans les cas particuliers où aucune application tierce ne peut résoudre le problème, il convient de développer une solution appropriée ou de suivre les recommandations du ch. 3.3 afin de satisfaire aux exigences.

5) *La sauvegarde des données de journalisation est-elle considérée comme un stockage séparé au sens de l'art. 4, al. 5, OPDo ?*

Une sauvegarde des données de journalisation serait déjà suffisante pour satisfaire à l'exigence d'utiliser un stockage séparé, tel que prévu à l'art. 4, al. 5, OPDo. Outre le renforcement de la protection contre d'éventuelles attaques, le stockage séparé a pour but d'éviter le chiffrement de ces données en cas d'incident lié à un rançongiciel.

6) *L'exécution de scripts d'automatisation doit-elle également être journalisée?*

Oui, si ces scripts peuvent enregistrer, modifier, lire, communiquer, effacer ou détruire des données personnelles. L'objectif de la journalisation est de pouvoir garantir la traçabilité des processus de traitement des données. Cela peut consister par exemple à enregistrer l'heure de début, l'heure de fin, la version du script, ou encore l'identité de la personne qui effectue le traitement.

7) *Qu'en est-il des appareils stockage en réseau (NAS), des réseaux de stockage (SAN) et des autres espaces de stockage de données ? Exemple : ouvrir un document Word*

*à partir du répertoire O:\Service_A\Donnees\Registre\xy.docx. Ces accès doivent-ils être journalisés ?*

L'art. 4, al. 2, OPDo doit être compris en relation avec l'art. 3, al. 3, let. a, OPDo, comme suit : l'obligation de journalisation s'applique uniquement aux données personnelles dans des systèmes de traitement automatisé des données. Dans le scénario décrit dans la question, il n'est donc pas obligatoire de journaliser les accès.

8) *Tous les procès-verbaux de journalisation doivent-ils être stockés au même endroit ?*

Pas nécessairement. Ce n'est en outre pas réaliste. Pour la journalisation, il est important que les procès-verbaux de journalisation soient disponibles et qu'ils puissent être regroupés de manière judicieuse. Les procès-verbaux de journalisation de pare-feu peuvent par exemple être stockés à un autre endroit que de l'Active Directory, tant que les modifications et les accès aux données personnelles restent reconstituables. La sécurité de l'information exige en outre que les procès-verbaux puissent être regroupés de manière à permettre la détection d'anomalies.

9) *Est-il autorisé d'utiliser des services externes à la demande pour la gestion des procès-verbaux de journalisation ?*

Dans la mesure du possible, il convient de consulter le service juridique et le conseiller à la protection des données de l'entreprise, car les risques dans le domaine des données personnelles ont plutôt tendance à augmenter qu'à diminuer. Nous déconseillons de recourir à de tels services. Une telle solution est exceptionnellement possible si on recourt déjà à un logiciel en tant que service (software-as-a-service) pour le traitement des données, à condition que les personnes susmentionnées aient déjà été consultées.

10) *Les métadonnées de chaque document contiennent également des données personnelles (des collaborateurs concernés) liées à la création du document, aux modifications et aux commentaires. Nous partons du principe que ces données personnelles ne sont pas visées par la journalisation prévue à l'art. 4 OPDo.*

Oui, c'est exact. Le but de la journalisation est de protéger les données personnelles traitées (c'est-à-dire contenues dans un document). Le fait que de nouvelles données personnelles soient générées suite au traitement de ces données personnelles (parce que la personne X a créé, modifié, etc. le document) ne requiert pas une nouvelle journalisation. Les données personnelles générées en vue de la traçabilité du traitement des données ne font pas elles-mêmes l'objet d'une journalisation.