



Registre des activités de traitement des données personnelles

(Article 31 du règlement 2018/1725)

Date : 7/05/2021

Numéro de référence : 176

Journaux d'évènements (log files) de l'environnement opérationnel de la DTI

Domaine d'activité : Activité administrative

Coordonnées

<i>Responsable du traitement ou Responsables conjoints du traitement :</i>	Direction des technologies de l'information, Cour de Justice de l'Union européenne, L-2925 Luxembourg	<i>Délégué à la protection des données :</i> Contact DataProtectionOfficer@curia.europa.eu
<i>Coordonnées de contact :</i>	Helpdesk@curia.europa.eu	
<i>Service traitant :</i>	Unité Opérations et support aux utilisateurs. Sécurité des systèmes d'information.	
<i>Sous-traitant :</i>	Consultants externes et prestataire de services institutionnel de l'UE.	

Accessible au public

Description du traitement

1) Finalité du traitement

Les fichiers journaux d'évènements (log files) sont utilisés par les administrateurs système. Ils sont très utiles et représentent un outil de travail indispensable afin de comprendre et suivre le comportement d'un système informatique. En tant que tel, les fichiers journaux d'évènements (log files) sont utilisés pour tracer les évènements dans un système d'information et pour aider lors de la réparation d'un débogage et lorsque les systèmes d'information ne fonctionnent pas correctement. Les fichiers journaux d'évènements (log files) font partie des systèmes et sont des outils essentiels pour assurer la sécurité informatique. Certains fichiers journaux d'évènements (log files) peuvent être utilisés pour des statistiques anonymes de connexions ou d'usage d'un système informatique.

2) Description du traitement

Le traitement est lié à l'exploitation et l'administration des serveurs, le stockage des données, les systèmes de télécommunications et en général de l'ensemble de l'infrastructure informatique de la Cour.

Les fichiers journaux d'évènements (log files) sont créés par les logiciels « système » pour tracer toute opération ou évènement d'un système. Ces éléments peuvent être le nom, le compte utilisateur (login ID), l'adresse logique (adresse IP). Un horodatage indiquant le début et la fin d'une opération. D'autres informations plus techniques sont également associées dans les journaux d'évènements mais ils ne sont pas des données personnelles. Elles sont collectées et utilisées pour comprendre le comportement du système.

Exemples de fichiers journaux:

- Logs lors de la connexion de proxy (accès vers des applications intranet et

	<p>Internet);</p> <ul style="list-style-type: none"> - Connexion aux serveurs Web (Server Log sert à garder la trace des processus de connexion: ouverture et fermeture connexion serveur); - Connexion a des serveurs middleware; - Enregistrement des connexions HTTP; - Les connexions aux bases des données (création de tables contenant des pistes d'audit).
--	--

<i>Catégorie de personnes concernées</i>	<i>Catégorie de données concernées</i>	<i>Durée de conservation des données</i>
Toute personne, qui utilise les systèmes d'information de la Cour de Justice peut avoir des traces de son compte utilisateur enregistré dans un fichier journal d'évènements (log files).	Enregistrement des comptes utilisateurs (login ID), les adresses IP, le temps d'ouverture de session, le temps de fermeture de session et le programme utilisé. Dans certains cas, le déroulement des actions exécutées sur le système d'information est également enregistré.	Les données sont conservées pour une durée maximale de 90 jours..

3) Destinataires	
<i>a) Au sein de l'institution</i>	Fonctionnaires de la DTI en charge du système d'information: les administrateurs système, y compris les administrateurs de bases de données et du réseau.

Accessible au public

	<p>Les données sont accessibles par les administrateurs de systèmes de l'infrastructure, et les sous-traitants de services informatiques. Les sous-traitants de services informatiques opèrent dans le cadre de contrats de service et travaillent à la Cour.</p> <p>Responsable de la sécurité des systèmes d'information et membres de l'équipe.</p>
<i>b) À l'extérieur de l'institution</i>	Dans des cas particuliers et pour des raisons de support, certains journaux peuvent être envoyés à des fournisseurs externes. Le personnel du prestataire de services.
4) <i>Transfert à un pays tiers ou une organisation internationale</i>	Néant
5) <i>Mesures de sécurité</i>	Les mesures de sécurité et les bonnes pratiques sont dérivées de la famille de normes ISO /IEC 27000 pour les systèmes de gestion de la sécurité de l'information.
6) <i>Notice d'information</i>	La notice d'information concernant ce traitement est accessible sur le site Intranet de la Cour.
7) <i>Limitations des droits</i>	Néant