IG HOSTING SWICO:
Guide pour les requêtes des autorités concernant les informations et contenus clients

PRÉAMBULE

Swico a élaboré ce guide pour les requêtes des autorités concernant les informations et contenus clients («Guide») en vue de présenter aux hébergeurs suisses les principes de comportement adaptés aux nouvelles technologies pour gérer les requêtes des autorités et des tribunaux suisses concernant les activités, les informations et les contenus des clients*. Les hébergeurs (et autres fournisseurs de services Internet) jouent un rôle indispensable pour la communication via Internet et donc pour l'économie, la société et la politique. En tant qu'intermédiaires, ils sont de plus en plus exposés à des réclamations de tiers privés ou d'autorités et de tribunaux en rapport avec les contenus que leurs clients rendent publiquement accessibles via Internet.

Le code de conduite Hébergement, qui est en place depuis 2013 et qui a fait ses preuves dans la pratique, contient des recommandations pour traiter les réclamations, notamment celles des entreprises ou des particuliers, à l'encontre des clients des hébergeurs. Le but de ce guide est de faciliter le traitement des requêtes des autorités et des tribunaux par les hébergeurs et de contribuer ainsi à l'amélioration de la sécurité juridique sur Internet.

Avec les recommandations contenues dans le guide, Swico suit d'une part les règles applicables du droit suisse en matière de renseignements et de mise à disposition d'informations aux autorités et aux tribunaux. D'autre part, elle remplit le champ d'interprétation juridique avec des recommandations de comportement en réponse aux requêtes officielles et judiciaires. Le guide a pour but de servir d'aide d'orientation initiale aux prestataires pour classer les requêtes et y réagir de manière appropriée.

Contenu

* La forme masculine est utilisée dans ce document pour désigner tous les genres.

A. Principes

1. Les requêtes des autorités doivent être soumises par écrit.

Afin de protéger les droits légaux (par ex. protection des données) et contractuels (par ex. obligation de secrets) des clients, les hébergeurs ne communiquent les informations ou les contenus des clients que sur demande écrite. Pour les requêtes informelles (par ex. simples requêtes de police, oralement/par e-mail), ils exigent une décision écrite et signée de l'autorité responsable. Est considérée comme «décision» tout ordre d'une autorité dans un cas particulier qui est fondé sur le droit public de la Confédération, du canton ou de la commune et qui, par exemple, justifie, modifie ou annule des droits ou des obligations (par ex. ordonnance de production de pièces du ministère public, décision d'un tribunal suisse). Dans ce contexte, c'est le contenu du courrier qui est important, et non son intitulé. Dans le cas de simples requêtes policières ou verbales de mise à disposition d'informations ou de contenus concernant les clients, le fournisseur exige une décision correspondante du ministère public. Les coûts de la décision ne doivent pas être imputés au fournisseur. En revanche, des frais peuvent être encourus dans le cadre de la procédure de recours.

2. Seules les autorités suisses reçoivent des renseignements

L'ordre doit identifier l'autorité requérante et la base juridique sur laquelle l'autorité se fonde. On entend par «autorité» toute institution domiciliée en Suisse qui accomplit une tâche de droit public de la Confédération, des cantons ou des communes qui lui a été confiée et qui est dotée d'une compétence de décision correspondante (par ex. ministères publics, tribunaux, administration des douanes, administrations fiscales, etc.) La compétence en matière de traitement des requêtes des autorités peut résulter d'un grand nombre de décrets. Il n'incombe généralement pas au à l'hébergeur de vérifier la compétence de décision de l'autorité.

En fonction de l'obligation légale de secret, des règles restrictives s'appliquent aux autorités compétentes, par ex. dans le domaine du secret des télécommunications ou en cas de requêtes provenant de l'étranger: Si la demande concerne des informations couvertes par le secret des télécommunications (art. 43 LTC en liaison avec art. 321ter CP), la requête doit être effectuée par l'intermédiaire du Service de surveillance de la correspondance par poste et télécommunication (service SCPT) (art. 26 al. 2 OSCPT). Si le fournisseur a des doutes quant au fait que la demande concerne le secret des télécommunications, le service SCPT se chargera de fournir des renseignements.

Afin de ne pas s'exposer au risque de poursuites pénales pour transmission illicite de renseignements (art. 271 CP), l'hébergeur ne donne pas suite aux demandes directes provenant de l'étranger et renvoie le demandeur à l'entraide administrative ou judiciaire internationale. L'autorité étrangère doit faire appel à l'assistance d'une autorité suisse. Cette dernière peut demander qu'une décision écrite soit rendue à l'encontre du fournisseur suisse. Dans des cas exceptionnels, les autorités étrangères peuvent adresser des requêtes directement aux hébergeurs suisses (sur la base de l'art. 32 let. b de la Convention sur la cybercriminalité). Toutefois, la mise à disposition directe de données d'inventaire et de données secondaires à l'étranger ne peut pas être imposée juridiquement en dehors de l'entraide administrative ou judiciaire internationale. Une mise à disposition directe volontaire n'est autorisée que si l'hébergeur y est habilité par le client sur la base d'une autorisation contractuelle.

3. Les requêtes imprécises doivent être clarifiées par les autorités

Les requêtes des autorités doivent décrire clairement les mesures requises de l'hébergeur et doivent être proportionnées, c'est-à-dire concrètement limitées (par ex. renseignements concernant des questions concrètes, mise à disposition et divulgation d'informations ou de données concernant des données spécifiques du détenteur ou des contenus spécifiques ainsi qu'en relation avec certains clients, noms de domaine, contenus clairement définis, périodes, etc.) Ce n'est pas aux fournisseurs de sélectionner les données concernées par une requête. La requête doit être formulée de manière suffisamment précise pour que le fournisseur puisse extraire les informations concernées sans ambiguïté et sans devoir faire sa propre sélection. Les fournisseurs demandent des précisions à l'autorité requérante si la formulation est ambiguë. Les fournisseurs n'ont pas à interpréter eux-mêmes les requêtes ambiguës. Dans le cas contraire, les hébergeurs courent le risque de devenir responsables des dommages causés à leurs clients ou aux tiers concernés.

4. Les hébergeurs sont des prestataires de services techniques

Les hébergeurs, comme les bureaux d'enregistrement, les fournisseurs de services de protection de la vie privée et les autres fournisseurs de services Internet, ne sont que des prestataires de services techniques pour leurs clients. Ils ne sont pas responsables des contenus de leurs clients (par ex. sites Internet, enregistrements de noms de domaine) en vertu du droit civil ou pénal, à moins qu'ils ne participent activement aux actions incriminées de leurs clients. Les données des détenteurs de noms de domaine et les données des exploitants de sites Internet sont en partie accessibles au public (par ex. Whois, mentions légales). Les hébergeurs informent les autorités requérantes sur leur rôle en tant que fournisseurs de services et, le cas échéant, les orientent vers des sources d'information accessibles au public sur les données de leurs clients.

5. Les hébergeurs et les autorités déterminent le mode de transfert de données approprié

Si les hébergeurs sont tenus de fournir des contenus ou des données, ils conviennent avec l'autorité ou la juridiction requérante des modalités techniques d'un transfert de données approprié et adapté aux circonstances, c'est-à-dire sécurisé. Ce faisant, les fournisseurs tiennent compte de l'état actuel de la technique, du caractère sensible et de l'étendue des données. Les informations librement accessibles à partir d'autres sources publiques (par ex. données de détenteurs dans Whois, mentions légales) peuvent être envoyées aux représentants des autorités par e-mail, à condition que la requête écrite réponde aux exigences du présent guide. Les contenus des clients qui ne sont pas accessibles au public doivent être cryptés et mis à disposition via un accès protégé.

Des procédures normalisées conformes à la LSCPT et les instructions spécifiques du service SCPT s'appliquent à la fourniture de renseignements et à la surveillance dans le secteur des télécommunications.

6. Les autorités attirent l'attention des hébergeurs sur une interdiction de communiquer

Si l'autorité requérante impose une interdiction de communiquer, l'hébergeur n'informe pas le client de la demande des autorités ni des mesures prises (interdiction de *fuiter des données*). Toute modification de la relation avec le client susceptible d'indiquer la mesure des autorités doit être évitée. Il appartient à l'autorité requérante de délivrer une interdiction de communiquer écrite en conséquence. Malgré l'interdiction de communiquer, il est possible que le client

concerné remarque des accès/modifications de son profil et puisse conclure de lui-même que des mesures correspondantes ont été prises.

7. Les contrats avec les clients restent en principe valables

En l'absence d'autres instructions des autorités concernées, les dispositions contractuelles entre l'hébergeur et le client restent inchangées. Les commandes des clients doivent continuer à être exécutées. Si l'hébergeur soupçonne des activités ou des contenus illicites du client, il peut (temporairement), à sa propre discrétion, suspendre ses propres services ou bloquer les contenus du client, à condition qu'il soit autorisé à le faire en vertu de ses propres dispositions contractuelles (par ex. conditions générales de vente, «CGV»). Tout ordre des autorités concernant des ordonnances de production de pièces (par ex. blocage de sous-pages, blocage de l'accès aux comptes clients) doit se conformer aux principes de ce guide. En cas d'interdiction de communiquer, le prestataire doit consulter au préalable l'autorité qui a ordonné la mesure s'il souhaite mettre fin à la relation avec le client.

8. Les hébergeurs doivent documenter et facturer leurs coûts

Les coûts s'orientent sur les bases juridiques respectives de la requête de l'autorité. Pour les mesures complexes, l'hébergeur discutera si possible à l'avance et de manière proactive de la réglementation des coûts avec l'autorité. Le fournisseur documente les coûts à prévoir ou déjà encourus. Le fournisseur ne peut pas facturer les coûts dans tous les cas.

IG HOSTING SWICO:
EXEMPLES DE REQUÊTES DES AUTORITÉS

1) Ordonnances de production de pièces dans les procédures pénales

a) *Objet*	Acquisition de documents et documentations exploitables du client directement par l'intermédiaire de l'hébergeur. Les hébergeurs sont les prestataires de services du client et stockent les contenus du client sur leurs serveurs. Les fournisseurs ont donc un pouvoir de disposition sur les données, même s'ils n'en sont pas propriétaires.
b) *Autorité requérante*	• Ministère public; • Si les informations demandées sont couvertes par le secret des télécommunications, les requêtes sont faites par l'intermédiaire du service SCPT. Si le fournisseur a des doutes quant au fait que la demande concerne le secret des télécommunications, le service SCPT se chargera de fournir des renseignements.
c) *Forme de l'ordre*	Décision écrite et signée
d) *Base juridique*	Art. 265 du Code de procédure pénale («CPP»; évent. avec référence au séquestre dans l'art. 263 CPP),
e) *Contenu*	• Spécification de la relation client concernée: par ex. personne concernée/accusée, client, relation client, nom de domaine, site Internet; • Indication de l'infraction pénale concernée ou de la procédure dans le cadre de laquelle l'ordonnance de production de pièces a lieu; • En cas de demande de renseignements: Catalogue de questions sans besoin d'interprétation pour le fournisseur; • Dans le cas d'une demande de mise à disposition: désignation concrète des documents, dossiers, fichiers, éventuellement données d'accès au compte client; • Brève justification de l'ordre, y compris base juridique; • Délai de renseignement/de mise à disposition (généralement prolongeable); • Évent. interdiction de communication de l'hébergeur avec le client

	• Sanctions possibles en cas d'infraction contre la décision (si avertissement dans la décision) Amendes jusqu'à CHF 10 000 (art. 292 en liaison avec art. 106, al. 1, du Code pénal «CP»), mesures de contraintes telles que perquisitions.
f) *Recours*	Les ordonnances de production de pièces ne sont pas contestables pour le fournisseur, des objections peuvent être formulées dans le cadre du droit de mise sous scellés.
g) *Possibilité de protéger les intérêts de l'hébergeur ou d'un tiers (par ex. clients)*	• Exiger la clarification des demandes de renseignements et de mises à disposition peu claires et ne publier le contenu que dans le cas de demandes d'information clairement définies; • Demander une prolongation du délai le cas échéant; • Réduire les renseignements et la mise à disposition à la mesure explicitement requise, mais ne pas procéder soi-même à une sélection/restriction; • Si les mesures ci-dessus ne sont pas suffisantes: la mise sous scellés d'informations et de documents est nécessaire s'il existe des droits de refus de témoigner ou d'autres intérêts de secret protégés par la loi (par ex. secrets professionnels des ministres du culte, des notaires, des auditeurs, des avocats, des médecins, secret bancaire des prestataires de services financiers, secret postal et de télécommunication des prestataires de services postaux et de télécommunication, protection des sources médiatiques). L'autorité concernée doit ensuite demander la levée des scellés par le biais du tribunal des mesures de contrainte afin de pouvoir consulter et exploiter les documents, dossiers, etc., concernés (art. 248 CPC). Si le fournisseur a demandé la mise sous scellés, il a la qualité de partie dans la procédure de levée des scellés. En principe, il appartient à l'autorité d'ordonner le renseignement et la mise à disposition de manière à ce que les intérêts de confidentialité et les droits de refus soient pris en compte.

IG HOSTING SWICO:
Guide pour les requêtes des autorités concernant les informations clients et contenus

* La forme masculine est utilisée dans ce document pour désigner tous les genres.

2) Ordonnances de production de pièces dans les procédures civiles

a) *Objet*	Acquisition de documents et documentations exploitables du client directement par l'intermédiaire de l'hébergeur. Les hébergeurs sont les prestataires de services du client et stockent les contenus du client sur leurs serveurs. Les fournisseurs ont donc un pouvoir de disposition sur les données, même s'ils n'en sont pas propriétaires.
b) *Autorité requérante*	Tribunaux
c) *Forme de l'ordre*	Jugement/décision d'instruction écrit/e et signé/e
d) *Bases légales*	Art. 160ss du Code de procédure civile («CPC»)
e) *Contenu*	• Spécification de la relation client concernée: par ex. client, relation client, nom de domaine, site Internet; • Information sur l'obligation de collaborer, les droits de refuser de collaborer et les conséquences du défaut (art. 161 CPC); • Indication de la personne concernée par la procédure dans le cadre de laquelle l'ordonnance de production de pièces a lieu; • Désignation concrète des documents à mettre à disposition; • Brève justification de l'ordre, y compris base juridique; • Délai de mise à disposition (généralement prolongeable); • Sanctions possibles en cas d'infraction contre la décision (si avertissement dans la décision) Amendes jusqu'à CHF 10 000 (art. 292 en liaison avec art. 106, al. 1 du Code pénal «CP»), amendes d'ordre jusqu'à CHF 1000; mesures de contrainte; frais de justice occasionnés par le refus (art. 167 CPC).
f) *Recours*	En tant que décisions provisoires, les ordonnances de production de pièces ne sont susceptibles d'un recours distinct qu'en cas de préjudice irréparable, le fournisseur n'étant pas partie à la procédure conduisant à une décision finale.

g) *Possibilité de protéger les intérêts de l'hébergeur ou d'un tiers (par ex. clients)*	• Exiger la clarification des demandes de renseignements et de mises à disposition peu claires et ne publier le contenu que dans le cas de demandes d'information clairement définies; • Demander une prolongation du délai le cas échéant; • Réduire les renseignements et la mise à disposition à la mesure explicitement requise, mais ne pas procéder soi-même à une sélection/restriction; • L'hébergeur en tant que tiers peut refuser de collaborer s'il risque de s'exposer ou d'exposer un de ses proches à une poursuite pénale ou d'engager sa responsabilité civile ou celle de ses proches (art. 166 al. 1, let. a CPC).

IG HOSTING SWICO:
Guide pour les requêtes des autorités concernant les informations et contenus clients

* La forme masculine est utilisée dans ce document pour désigner tous les genres.

Exemples de requêtes des autorités

3) Ordre de surveillance des télécommunications

a) *Objectif et rôle des hébergeurs*	Les personnes soumises à la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication («LSCPT») ont une obligation de collaborer. Les catégories suivantes ont une obligation de collaborer: Les fournisseurs de services de télécommunication («FST») et les fournisseurs de services de communication dérivés («FSCD»). Les services de communication dérivés sont fondés sur des services de télécommunication et permettent une communication unilatérale ou multilatérale (art. 2 let. c LSCPT). La LSCPT examine séparément les différentes offres de services: un fournisseur peut être considéré comme un FST pour l'offre de service A, comme un FSCD pour l'offre de service B et ne pas avoir d'obligation de coopération pour l'offre de service C. Les FST et une partie des FSCD ont des obligations actives conformément à la LSCPT. Les autres fournisseurs ont seulement des obligations de tolérer. Chaque hébergeur doit préciser s'il entre dans le cadre de la LSCPT et à quelle catégorie d'obligations de collaborer il appartient. La «Notice FST-FSCD» sur le site Internet du service SCPT (version actuelle disponible à l'adresse: www.li.admin.ch > Thèmes > La nouvelle LSCPT > Notice FST-FSCD) sert de soutien. Les hébergeurs (par ex., hébergement purement physique) qui ne proposent pas de communication unilatérale ou multilatérale et d'accès à Internet ne relèvent pas des catégories FST et FSCD, ce qui signifie qu'ils n'ont généralement pas d'obligation de collaborer dans le cadre de la LSCPT. Cependant, les hébergeurs sont généralement considérés comme des FSCD. L'ordonnance (OSCPT) relative à la LSCPT distingue trois catégories de FSCD: 1. «FSCD ordinaire» (uniquement obligations de tolérer en matière de renseignements et de surveillance); 2. «FSCD ayant des obligations étendues en matière de fourniture de renseignements» (art. 22 al. 4 LSCPT et art. 22 OSCPT, obligations de renseignements actives et identification des usagers): selon décision du Service SCPT, si

	• au moins 100 demandes de renseignements ont été formulées au cours des 12 derniers mois (date de référence: 30 juin), *ou si* • le chiffre d'affaires annuel en Suisse au cours de deux exercices consécutifs est respectivement d'au moins 100 millions de CHF, une grande partie de l'activité commerciale consiste à fournir des services de communication dérivés, et au moins 5000 usagers utilisent les services des fournisseurs; 3. «FSCD ayant des obligations étendues en matière de surveillance» (art. 27, al. 3, LSCPT et art. 52 OSCPT, obligations de surveillance actives, y compris conservation des données, c'est-à-dire conservation des données secondaires pendant 6 mois): Selon décision du service SCPT si • des mandats de surveillance ont été effectués au cours des 12 derniers mois pour au moins 10 objectifs de surveillance différents (date de référence: 30 juin), ou si • le chiffre d'affaires annuel en Suisse au cours de deux exercices consécutifs est respectivement d'au moins 100 millions de CHF, une grande partie de l'activité commerciale consiste à fournir des services de communication dérivés, et au moins 5000 usagers utilisent les services des fournisseurs.
b) *Autorité requérante*	L'interlocuteur des hébergeurs est le Service de surveillance de la correspondance par poste et télécommunication («Service SCPT»). Il est chargé d'initier, de contrôler et d'effectuer une surveillance des télécommunications et reçoit les renseignements des fournisseurs. La requête du service SCPT se base sur l'ordre d'une autorité de poursuite pénale (généralement un ministère public, en cas de surveillance autorisée par le tribunal des mesures de contrainte). Si le fournisseur a des doutes quant au fait que la demande concerne le secret des télécommunications, le service SCPT se chargera de fournir des renseignements.
c) *Forme de l'ordre*	• Pour les renseignements: décision écrite et signée de l'autorité de poursuite pénale; • Pour les surveillances: décision écrite et signée (et approuvée dans les cinq jours par le tribunal des mesures de contrainte) de l'autorité de poursuite pénale;

	• Décision écrite et signée du service SCPT uniquement si l'hébergeur la réclame ou porte atteinte à l'obligation de coopération; • Envoi de la demande/ordre et transmission des données: Via le système de traitement exploité par le service SCPT.
d) *Bases légales*	LSCPT et art. 269 ss. CPP, Ordonnance sur la surveillance de la correspondance par poste et télécommunication («OSCPT»), Ordonnance du DFJP sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication («OME-SCPT»), Ordonnance sur les émoluments et les indemnités en matière de surveillance de la correspondance par poste et télécommunication («OEI-SCPT»).

e) *Contenu*	• Spécification de la relation client concernée: par ex. personne concernée/accusée, client, relation client, nom de domaine, site Internet, adresse IP, identification de l'usager (nom d'utilisateur);
	• Brève justification avec toutes les informations nécessaires à la surveillance ou à la fourniture de renseignements;
	• Indication de la période concernée;
	• Indication de la base juridique;
	• Hébergeur en tant que FSCD ordinaire (cas normal):
	  • Obligation de tolérer concernant les mesures de surveillance des données transmises ou enregistrées par le client surveillé (art. 27, al. 1 LSCPT): Le fournisseur doit accorder l'accès aux installations (par ex. bâtiments, équipements, réseaux, services) et fournir les renseignements nécessaires à la surveillance;
	  • Fourniture sur demande des données secondaires disponibles du client surveillé (surveillances rétroactives, art. 27 al. 2 LSCPT);
	  • Renseignement sur les informations disponibles afin d'identifier les auteurs des délits commis via Internet et d'identifier les personnes en cas de menaces internes ou externes (art. 22, al. 3 LSCPT, données d'inventaire);

	• Renseignements concernant les informations à disposition (art. 18 al. 5 OSCPT) sur les clients de services de communications dérivés (par ex. art. 43 OSCPT): en particulier données relatives aux usagers (par ex. numéro de client, nom d'utilisateur) et informations permettant d'identifier l'usager (informations sur la personne physique ou morale, coordonnées, sexe de la personne physique), identification du service concerné, période (activation, fin d'utilisation), statut et blocage antérieur éventuel, éléments d'adressage et autres identificateurs; • Renseignements concernant les informations à disposition (art. 18 al. 5 OSCPT) sur les clients de services de courrier électronique (art. 42 OSCPT): en particulier données relatives aux usagers (par ex. nom d'utilisateur) et informations permettant d'identifier l'usager (informations sur la personne physique ou morale, coordonnées, sexe de la personne physique), service de courrier électronique, adresse e-mail, période (activation, fin d'utilisation), éléments d'adressage (alias de messagerie); listes de diffusion; • Renseignements sur les données à disposition (art. 18, al. 5 OSCPT) sur la méthode de paiement (art. 44 OSCPT): en particulier mode de paiement (débit, virement, prépayé), coordonnées bancaires du client, adresse de facturation; • Copies des factures disponibles du client (art. 46 OSCPT); • Copies des documents contractuels disponibles du client (art. 47 OSCPT). • Hébergeur en tant que FSCD avec obligations de renseignements complémentaires (en plus): • Renseignements sur les clients de services de communications dérivés (par ex. art. 43 OSCPT): en particulier données relatives aux usagers (par ex. numéro de client, nom d'utilisateur) et informations permettant d'identifier l'usager (informations sur la personne physique ou morale, coordonnées, sexe de la personne physique), identification du service concerné, période (activation, fin d'utilisation), statut et blocage antérieur éventuel, éléments d'adressage et autres identificateurs;

	• Renseignements sur les clients de services de courrier électronique (art. 42 OSCPT): en particulier données relatives aux usagers (par ex. nom d'utilisateur) et informations permettant d'identifier l'usager (informations sur la personne physique ou morale, coordonnées, sexe de la personne physique), service de courrier électronique, adresse e-mail, période (activation, fin d'utilisation), éléments d'adressage (alias de messagerie); listes de diffusion; • Renseignements sur la méthode de paiement (art. 44 OSCPT): en particulier le mode de paiement (débit, virement, prépayé), coordonnées bancaires du client, adresse de facturation; • Copies des factures disponibles du client (art. 46 OSCPT); • Copies des documents contractuels disponibles du client (art. 47 OSCPT). • Hébergeur en tant que FST ou FSCD avec obligations de surveillance complémentaires (en plus): • Surveillance en temps réel ou surveillance rétroactive des données secondaires de services de courrier électronique (art. 58, 59 et 62 OSCPT): en particulier, date et heure des procédures de connexion et de déconnexion, statut de l'identificateur de l'usager, alias de messagerie, adresse IP, numéros de port, volume de données, adresse e-mail de l'expéditeur et du destinataire, • Surveillance en temps réel du contenu des services de courrier électronique (art. 59 OSCPT). • Les délais sont régis par l'Ordonnance du DFJP sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication («OME-SCPT»); • Remarque concernant l'obligation de confidentialité: la surveillance ou la fourniture de renseignement doit être effectuée de manière à ce que la personne surveillée ou des tiers non autorisés n'en aient pas connaissance; • Menace de sanctions en cas d'infraction contre une décision du service SCPT ou de non-respect des obligations (par ex. violation de l'obligation de secret): Amendes jusqu'à CHF 100 000 (art. 39, al. 1 LSCPT), ou plus si une infraction plus grave est commise;

	• Indications des voies de recours.
f) *Recours*	Les hébergeurs peuvent, dans un délai de 30 jours, former un recours auprès du Tribunal administratif fédéral contre les décisions du service SCPT (art. 42 LSCPT en liaison avec art. 47, al. 2, let. b et 50 LCA), dans la mesure où il s'agit d'ordonnances techniques ou organisationnelles du service SCPT. Dans ce recours, les fournisseurs ne peuvent faire valoir que les conditions (de procédure pénale) permettant (à l'autorité de poursuite pénale) d'ordonner une surveillance ne sont pas remplies.
g) *Possibilité de protéger les intérêts de l'hébergeur ou d'un tiers (par ex. clients)*	• Exiger la clarification des demandes de renseignements et de mises à disposition peu claires et ne publier les contenus que dans le cas de demandes d'information clairement définies; • Les informations couvertes par le secret des télécommunications ne peuvent être publiées que si la demande a été transmise par le service SCPT; • Demander une prolongation du délai le cas échéant; • Réduire les renseignements et la mise à disposition à la mesure explicitement requise, mais ne pas procéder soi-même à une sélection/restriction; • En cas de questions ou de doutes, le service SCPT fournit volontiers des renseignements.
h) *Coûts*	L'OEI-SCPT réglemente l'indemnisation des personnes obligées de collaborer pour les frais d'une surveillance. Les hébergeurs concernés peuvent facturer au service SCPT dès qu'ils ont confirmé l'exécution de la commande ou fourni les renseignements demandés. Ils établissent une facture détaillée par mois civil et la transmettent au service SCPT au plus tard le quinzième jour ouvrable du mois suivant (art. 5 OEI-SCPT).

	• Indications des voies de recours.
f) *Recours*	Les hébergeurs peuvent, dans un délai de 30 jours, former un recours auprès du Tribunal administratif fédéral contre les décisions du service SCPT (art. 42 LSCPT en liaison avec art. 47, al. 2, let. b et 50 LCA), dans la mesure où il s'agit d'ordonnances techniques ou organisationnelles du service SCPT. Dans ce recours, les fournisseurs ne peuvent faire valoir que les conditions (de procédure pénale) permettant (à l'autorité de poursuite pénale) d'ordonner une surveillance ne sont pas remplies.
g) *Possibilité de protéger les intérêts de l'hébergeur ou d'un tiers (par ex. clients)*	• Exiger la clarification des demandes de renseignements et de mises à disposition peu claires et ne publier les contenus que dans le cas de demandes d'information clairement définies; • Les informations couvertes par le secret des télécommunications ne peuvent être publiées que si la demande a été transmise par le service SCPT; • Demander une prolongation du délai le cas échéant; • Réduire les renseignements et la mise à disposition à la mesure explicitement requise, mais ne pas procéder soi-même à une sélection/restriction; • En cas de questions ou de doutes, le service SCPT fournit volontiers des renseignements.
h) *Coûts*	L'OEI-SCPT réglemente l'indemnisation des personnes obligées de collaborer pour les frais d'une surveillance. Les hébergeurs concernés peuvent facturer au service SCPT dès qu'ils ont confirmé l'exécution de la commande ou fourni les renseignements demandés. Ils établissent une facture détaillée par mois civil et la transmettent au service SCPT au plus tard le quinzième jour ouvrable du mois suivant (art. 5 OEI-SCPT).

IG HOSTING SWICO:
Guide pour les requêtes des autorités concernant les informations et contenus clients

* La forme masculine est utilisée dans ce document pour désigner tous les genres.

Exemples de requêtes des autorités

4) Interrogatoire (audition) de personnes physiques

a) *Objet*	Renseignement fournis par des personnes physiques occupant un poste de direction chez l'hébergeur sur les procédures relatives aux contenus des clients. La personne physique est interrogée en tant que témoin.
b) *Autorité requérante*	En fonction du domaine juridique concerné, par ex. tribunal, ministère public
c) *Forme de l'ordre*	Décision écrite et signée (convocation)
d) *Base juridique*	En fonction du domaine juridique concerné (par ex. art. 160 et 170 CPC ou art. 177 CPP pour les témoins, art. 190 al. 2 ou art. 145 CPP pour les renseignements écrits ou les rapports écrits)
e) *Contenu*	• Spécification de la relation client concernée: par exemple, personne concernée/accusée, client, relation client, nom de domaine, site Internet; • Indication de l'infraction pénale concernée ou de la procédure dans le cadre de laquelle l'ordonnance de production de pièces a lieu (par ex. entraide administrative des autorités étrangères); • Par exemple convocation de personnes ayant le statut d'organe comme témoins, demande d'un rapport écrit; • En cas de demande d'un rapport écrit: catalogue de questions sans besoin d'interprétation pour le fournisseur; • Brève justification de l'ordre ou au moins indication de la base juridique; • Date de l'interrogatoire ou date limite pour le rapport (généralement décalable);

	• Pendant l'interrogatoire (audition): Menace de sanction en cas de faux témoignage (à condition que cela soit signalé dans la convocation): peine d'emprisonnement ou amende (art. 307 CP); • Pendant l'interrogatoire (audition): référence au droit de refus de témoigner et au devoir de vérité (art. 160, 166 et 171 CPC, art. 168 ss, 177 CPP, art. 307 CP).
f) *Recours*	Les convocations à un interrogatoire ou les demandes de renseignements ou de rapports écrits ne sont pas contestables par le fournisseur.
g) *Possibilité de protéger les intérêts de l'hébergeur ou d'un tiers (par ex. clients)*	• Exiger la clarification des demandes de renseignements et de mises à disposition peu claires et ne publier les contenus que dans le cas de demandes d'information clairement définies; • Demander une prolongation du délai le cas échéant; • Réduire les renseignements et la mise à disposition à la mesure explicitement requise, mais ne pas procéder soi-même à une sélection/restriction; • Les hébergeurs en tant que tiers peuvent refuser de collaborer ou de témoigner, par ex. s'ils risquent de s'exposer ou d'exposer un de leurs proches à une poursuite pénale ou d'engager leur responsabilité civile ou celle de leurs proches (art. 166 al. 1, let. a CPC ou art. 169 CPP) ou s'ils sont étroitement liés à une partie / un accusé (par ex. en ligne droite ou en ligne collatérale jusqu'au troisième degré ou parents par alliance, en partenariat de vie effectif, avec des enfants communs). Si des droits de refus de témoigner existent, la personne physique peut refuser de témoigner.

IG HOSTING SWICO:
Guide pour les requêtes des autorités concernant les informations et contenus clients

* La forme masculine est utilisée dans ce document pour désigner tous les genres.

Exemples de requêtes des autorités

5) Actions d'une autorité ou d'un mandataire à la place du client

a) *Objet*	S'assurer que l'hébergeur n'accepte plus les instructions des anciens interlocuteurs du client, mais agit uniquement sur instruction de l'autorité ou de la personne mandatée. L'hébergeur est le prestataire de services du client et une autre personne autorisée est désormais habilitée à donner des instructions à sa place.
b) *Autorité requérante*	Selon le domaine juridique concerné, par ex. l'autorité de surveillance, la personne mandatée par l'autorité (par ex. l'enquêteur, le cabinet d'avocats, le cabinet de conseil, le liquidateur, l'administrateur de la faillite).
c) *Forme de l'ordre*	Ordre écrit et signé ou lettre de la personne mandatée, accompagné d'une décision exécutoire correspondante (par ex. décision de justice, décision relative aux mesures superprovisionnelles et préventives).
d) *Base juridique*	En fonction du domaine juridique concerné
e) *Contenu*	• Spécification de la relation client concernée: par ex. personne concernée/accusée • Client, relation client, nom de domaine, site Internet; • Indication de l'infraction pénale concernée ou de la procédure dans le cadre de laquelle l'ordonnance de production de pièces du client a lieu (par ex. procédure de surveillance, procédure de faillite); • Message de l'autorité ou de la personne mandatée selon lequel les personnes de contact actuelles ne sont plus autorisées à disposer du compte utilisateur et des contenus du client et l'hébergeur ne peut agir que sur instruction de l'autorité/de la personne autorisée;

	• Joindre une décision exécutoire correspondante (par ex. un jugement) en vertu de laquelle l'autorité/personne requérante est autorisée à agir à la place des organes de l'entreprise concernée); • Évent. instructions d'actions concrètes: par ex. fourniture de renseignements, refus des instructions des clients concernés et de leurs organes, blocage des accès clients, sécurisation des contenus; • Délais; • Év. conséquences des sanctions (en fonction du droit applicable)
f) *Recours*	En général, aucun pour l'hébergeur, car il n'est pas partie à la procédure.
g) *Possibilité de protéger les intérêts de l'hébergeur ou d'un tiers (par ex. clients)*	• Exiger des précisions sur les ordres ou demandes de renseignements et de mise à disposition peu clairs. N'accorder l'accès ou mettre à disposition les contenus que si la demande est précisément délimitée; • Si nécessaire, exiger une prolongation du délai pour des mesures individuelles concrètes; • Réduire l'accès, les renseignements et la mise à disposition à la mesure explicitement requise, mais ne pas procéder soi-même à une sélection/restriction.