# Directive du DFJP sur la mise en place de liaisons en ligne et l'octroi d'autorisations d'accès à des applications informatiques du DFJP

**(Directive du DFJP sur les liaisons en ligne)**

du 30 septembre 2004

*Le Département fédéral de justice et police,*

vu l'art. 38 de la loi fédérale du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[1],

*arrête:*

## Section 1 Généralités

### Art. 1 But

[1] La présente directive vise à harmoniser la procédure lors de la mise en place de liaisons en ligne au Département fédéral de justice et police (DFJP).

[2] Elle fixe:

a. la procédure et les conditions de mise en place d'une liaison en ligne entre le DFJP et des organes de la Confédération et des cantons, qui permet aux employés de ces organes (utilisateurs) d'avoir accès, par une procédure d'appel, à une application informatique du DFJP;

b. la procédure et les conditions d'octroi d'une autorisation d'accès individuelle ou collective à ces utilisateurs lorsque des données personnelles leur sont rendues accessibles au moyen de cette liaison en ligne.

### Art. 2 Conditions

L'autorisation de mettre en place une liaison en ligne entre une application informatique du DFJP et un utilisateur est assujettie à:

a. l'existence d'une base légale suffisante, conformément à l'art. 19, al. 3, de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[2], qui fixe concrètement les accès autorisés et les conditions générales qui les régissent (art. 3);

b. la conformité aux buts (art. 4);

1 RS **172.010**
2 RS **235.1**

c. la sécurité de la liaison en ligne (art. 5);

d. une demande de l'autorité cantonale compétente si la mise en place d'une liaison en ligne concerne un organe cantonal (art. 16).

## Section 2 Conditions de mise en place d'une liaison en ligne

### Art. 3 Base légale

Toute mise en place d'une liaison en ligne doit être fondée sur une base légale expresse. La base légale doit être une loi au sens formel si la liaison en ligne permet d'accéder à des données sensibles ou à des profils de la personnalité.

### Art. 4 Conformité aux buts

1 Une liaison en ligne ne doit être mise en place qu'aux fins prévues par la base légale.

2 Si la base légale définit le but uniquement de manière générale, la demande de mise en place d'une liaison en ligne devra le décrire de manière plus précise.

### Art. 5 Sécurité

1 Une liaison en ligne ne peut être installée que si le traitement correct des données et la sécurité des données sont assurés, c'est-à-dire que les mesures techniques visées à la section 3 sont réalisées.

2 Une infrastructure de sécurité centralisée (portail SSO du DFJP[3]) contrôle l'accès à toutes les informations et applications informatiques du DFJP. Le portail SSO du DFJP permet d'assurer une gestion standardisée et une authentification stricte des utilisateurs.

## Section 3 Mesures techniques et organisationnelles

### Art. 6 Appréciation des risques

Avant la mise en place d'une application informatique contenant une liaison en ligne, l'office fédéral responsable de l'application informatique doit effectuer une appréciation des risques, conformément aux directives en matière de sécurité informatique du Conseil de l'informatique de la Confédération (CI) et de l'Unité de stratégie informatique de la Confédération (USIC), et prendre les mesures qui s'imposent.

3 Single-Sign-On Portal DFJP

**Art. 7** Plan de sécurité de l'application informatique

[1] L'office fédéral responsable de l'application informatique établit, sur la base de l'appréciation des risques, un plan de sécurité de l'application exposant les mesures de sécurité nécessaires visées à l'art. 20 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD)[4].

[2] Le plan de sécurité de l'application informatique mentionne notamment:

a. les responsables de l'application;
b. les responsables de la protection des données;
c. les responsables de la sécurité informatique;
d. l'organe de contrôle;
e. les règles de journalisation;
f. la procédure d'identification et d'authentification des utilisateurs;
g. le chiffrement des données;
h. la procédure d'octroi des autorisations d'accès;
i. les règles et la procédure de mise hors service des liaisons inactives et de blocage des autorisations d'accès dont il n'est pas fait usage;
j. la procédure des contrôles visés à l'art. 9, al. 1, OLPD.

[3] Le plan de sécurité de l'application informatique est mis périodiquement à jour par l'office fédéral qui en est responsable.

[4] Le rapport final de sécurité établi avec le conseiller à la sécurité informatique du département (CSID) et l'Unité de stratégie informatique de la Confédération peut tenir lieu de plan de sécurité de l'application informatique si les points mentionnés à l'al. 2 figurent dans le règlement de traitement.

**Art. 8** Règlement de traitement

Conformément à l'art. 21 OLPD, les offices fédéraux responsables des applications informatiques établissent un règlement de traitement de leurs applications informatiques.

## Section 4
## Conditions d'octroi des autorisations d'accès individuelles

**Art. 9** Adéquation

L'accès en ligne doit permettre à l'utilisateur d'atteindre les buts concrets qu'il vise.

4 RS **235.11**

**Art. 10** Nécessité

1 L'accès en ligne doit être nécessaire pour accomplir une tâche fixée par la loi.

2 La nécessité d'obtenir un accès en ligne est réputée établie si l'exécution d'une tâche sans cet accès engendre pour l'utilisateur une charge de travail supplémentaire disproportionnée.

**Art. 11** Proportionnalité

1 L'accès en ligne doit être conforme au principe de proportionnalité.

2 Il répond au principe de proportionalité lorsqu'il existe un équilibre raisonnable entre l'atteinte à la personnalité des personnes concernées et les bénéfices escomptés du traitement des données.

3 L'accès en ligne individuel doit être limité aux données et aux fonctions dont l'utilisateur a besoin pour accomplir sa tâche.

**Art. 12** Critères d'appréciation

Lors de l'appréciation des principes mentionnés aux art. 9 à 11, la personne chargée d'octroyer les autorisations d'accès en ligne individuelles prend notamment en compte les critères suivants:

a. la fréquence prévisible de l'utilisation de chaque accès en ligne;

b. la fréquence d'utilisation à ce jour par l'organe fédéral ou cantonal concerné;

c. le nombre de collaborateurs de l'organe fédéral ou cantonal concerné ayant déjà une autorisation d'accès en ligne;

d. l'ampleur de l'accès en ligne accordé à l'organe fédéral ou cantonal concerné;

e. la nécessité d'agir rapidement et de manière indépendante (p. ex en dehors des heures de bureau);

f. l'ampleur de l'accès en ligne requis (critères de recherche, ampleur des données pouvant être visualisées);

g. les fonctions requises (interrogation, enregistrement, mutation, effacement).

## Section 5 Organisation

**Art. 13** Organe central d'authentification

1 L'organe central d'authentification (service d'authentification du DFJP) est chargé d'authentifier les utilisateurs qui sollicitent l'accès en ligne aux applications informatiques du DFJP. Il gère le portail SSO du DFJP.

2 Il reçoit les demandes d'accès en ligne, authentifie les bénéficiaires de ces accès et transmet les demandes à l'office fédéral responsable de l'application informatique.

3 Il coordonne la procédure d'octroi des autorisations d'accès en ligne individuelles.

**Art. 14** Compétences au sein de l'office fédéral responsable de l'application informatique

[1] Le conseiller à la protection des données de l'office fédéral responsable de l'application informatique (CPDO) surveille la planification et la mise en place des liaisons en ligne et veille au respect des règles d'octroi des autorisations d'accès en ligne individuelles.

[2] Il examine la première demande d'autorisation d'accès en ligne individuelle provenant de chaque organe de la Confédération ou des cantons et contrôle que les conditions définies à la section 4 sont remplies. Il vérifie, par sondage, que les autorisations suivantes sont accordées conformément aux art. 9 à 12.

[3] Il examine si le règlement de traitement est correct et complet.

[4] Le conseiller à la sécurité informatique de l'unité administrative (CSI-O) est responsable de l'examen des aspects liés à la sécurité informatique. Il examine notamment si les mesures de sécurité répondent aux exigences des art. 6 et 7.

**Art. 15** Fournisseur de prestations de l'application informatique

Le fournisseur de prestations de chaque application informatique est chargé de la réalisation technique des accès en ligne lorsque les demandes d'accès individuelles ont été approuvées.

## Section 6 Procédure de mise en place d'une liaison en ligne

**Art. 16** Demande de l'autorité cantonale compétente

L'autorité cantonale compétente transmet la demande de mise en place d'une liaison en ligne à l'office fédéral responsable de l'application informatique. La demande contient:

a. le nom des organes pour lesquels elle demande qu'une liaison en ligne soit mise en place;

b. le nom de l'application informatique à laquelle ces organes doivent avoir accès;

c. le but pour lequel la liaison doit être mise en place pour autant que la base légale définisse le but uniquement de manière générale.

**Art. 17** Examen de la demande de mise en place d'une liaison en ligne

[1] Le CPDO examine la demande; il contrôle notamment:

a. l'existence d'une base légale suffisante;

b. la conformité aux buts;

c. les demandes d'autorisation collective.

2 Si la demande est acceptée, il transmet le règlement de traitement de l'application informatique à l'autorité cantonale qui a fait la demande.

## Section 7
## Procédure d'octroi d'autorisations d'accès en ligne individuelles

**Art. 18** Demande d'autorisation d'accès

1 La demande d'autorisation d'accès individuelle doit être faite au moyen du formulaire du DFJP figurant sur Intranet ou Internet.

2 Elle doit être envoyée par voie électronique à l'organe central d'authentification.

**Art. 19** Examen des demandes d'autorisation d'accès en ligne individuelles

1 L'office fédéral responsable de l'application informatique examine les demandes d'autorisation d'accès en ligne individuelles selon les principes visés à la section 4.

2 Le CPDO examine la première demande d'autorisation d'accès en ligne individuelle transmise par un organe de la Confédération ou des cantons. Il contrôle par sondage les autorisations d'accès en ligne individuelles accordées par la suite à une personne appartenant au même organe.

3 L'office responsable de l'application informatique désigne les personnes habilitées à examiner les demandes suivantes. Il peut déléguer l'examen des demandes suivantes à des organes cantonaux.

**Art. 20** Autorisations collectives

1 Une autorisation collective permet à tous les utilisateurs appartenant au même groupe d'utilisateurs d'utiliser les mêmes paramètres d'identification pour la prise de contact (log in de groupe) avec le portail SSO du DFJP et les applications informatiques du DFJP.

2 Une autorisation collective peut être octroyée à certaines catégories d'utilisateurs lorsque les exigences de la section 4 sont satisfaites. En outre, les conditions suivantes doivent être remplies:

a. le poste de travail est utilisé en continu;

b. la connexion avec une application doit être établie très rapidement car l'accès est urgent;

c. le poste de travail peut être utilisé par toutes les personnes appartenant au groupe d'utilisateur mentionné dans la demande d'autorisation collective;

d. les détenteurs d'autorisations collectives ne peuvent que consulter les données d'un système d'information;

e. les plans de relève du groupe d'utilisateurs sont conservés durant une année;

f. la liste des membres du groupe d'utilisateurs est annoncée au responsable de l'application; et

g. les mutations au sein du groupe d'utilisateurs sont annoncées au moins deux fois par an au responsable de l'application.

**Art. 21** Surveillance

Le CPDO examine périodiquement si les accès accordés sont conformes aux principes énoncés à la section 4.

## Section 8 Dispositions finales

**Art. 22** Dispositions d'exécution

La présente directive figure en annexe et fait partie intégrante du règlement de traitement de chaque application informatique du DFJP contenant des liaisons en ligne.

**Art. 23** Dispositions transitoires

1 Les autorisations d'accès en ligne individuelles qui sont valables au moment de l'entrée en vigueur de la présente directive le demeurent jusqu'à l'introduction de la procédure d'authentification stricte des utilisateurs. Un réexamen des autorisations d'accès en ligne individuelles au sens de l'art. 19 sera effectué à ce moment-là.

2 Lorsqu'une nouvelle application informatique remplace une application existante, les autorisations de mettre en place une liaison en ligne (art. 17) demeurent valables.

3 Jusqu'à l'introduction de la signature électronique au DFJP, une reproduction sur papier, dûment signée, de la demande (art. 18, al. 1) doit être obligatoirement envoyée par fax ou par courrier postal à l'organe central d'authentification.

4 Le DFJP transmet jusqu'au 31 décembre 2004 les règlements de traitement des applications informatiques accessibles en ligne le 31 août 2004 aux autorités cantonales responsables des organes cantonaux qui y sont reliés.

**Art. 24** Entrée en vigueur

La présente directive entre en vigueur le 1er octobre 2004.

30 septembre 2004

Département fédéral de justice et police:

Christoph Blocher

# Directive du DFJP sur les liaisons en ligne et l'octroi d'autorisations d'accès à des applications informatiques du DFJP

| | |
|---|---|
| In<br>Dans<br>In | Bundesblatt<br>Feuille fédérale<br>Foglio federale |
| Jahr<br>Année<br>Anno | 2004 |
| Band<br>Volume<br>Volume | 1 |
| Heft<br>Cahier<br>Numero | 42 |
| Geschäftsnummer<br>Numéro d'affaire<br>Numero dell'oggetto | --- |
| Datum<br>Date<br>Data | 26.10.2004 |
| Seite<br>Page<br>Pagina | 5413-5420 |
| Ref. No | 10 138 079 |