

JUSTEL - Législation consolidée

http://www.ejustice.just.fgov.be/cgi_loi/change_lg_2.pl?language=fr&la=F&nm=2021031576

Dossier numéro : 2021-07-13/02

Titre

13 JUILLET 2021. - Directive contraignante commune des Ministres de la Justice et de l'Intérieur relative aux mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2 de la Loi sur la Fonction de Police

Source : JUSTICE

Publication : Moniteur belge du 13-07-2021 page : 70389

Entrée en vigueur : 23-07-2021

Table des matières

Art. M

Texte

Article M.

Directive contraignante commune des Ministres de la Justice et de l'Intérieur relative aux mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans les banques de données visées à l'article 44/2 de la Loi sur la Fonction de Police

A Mesdames et Messieurs les Bourgmestres,
Au Commissaire général de la police fédérale.

Pour information à :

Mesdames et Messieurs les Procureurs généraux,

Madame et Messieurs les Gouverneurs de province,

Monsieur le Ministre-Président de la Région de Bruxelles-Capitale,

Monsieur le Procureur fédéral et Mesdames et Messieurs les Magistrats du parquet fédéral,

Mesdames et Messieurs les Commissaires d'arrondissement,

Monsieur le Président de la Commission Permanente de la police locale,

Mesdames et Messieurs les Chefs de corps de la police locale,

Madame et Messieurs les Présidents de l'Organe de contrôle de l'information policière, du Comité permanent de contrôle des services de police et de l'Inspection générale de la police fédérale et de la police locale.

Madame le Bourgmestre,

Monsieur le Bourgmestre,

Monsieur le Commissaire général,

I. CADRE LEGAL ET CHAMP D'APPLICATION

L'article 44/4, § 2 de la loi sur la fonction de police (ci-après " LFP ") constitue la base légale pour la présente directive contraignante, portant sur les mesures nécessaires en vue d'assurer la gestion et la sécurité dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel et des informations traitées dans la banque de données nationale générale, les banques de données de base, les banques de données particulières, les banques de données communes et les banques de données techniques visées à l'article 44/2 de la LFP.

Bien que la présente directive traite en principe du contexte nécessaire pour la sécurité des systèmes opérationnels, cela n'exclut pas que, en complément de la LFP et du titre 2 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (ci-après " la loi

sur la protection des données " ou " LPD "), également le Règlement Général sur la Protection des Données¹ et le titre 1 de la LPD s'appliquent à certaines mesures prises en vertu de la présente directive.

La présente directive est applicable aux services de police au sens de l'article 2, 2° de la loi du 7 décembre 1998 organisant un service de police intégré structuré à deux niveaux.

L'avis du Conseil des bourgmestres a été donné le 12 août 2020, celui de l'Organe de contrôle de l'information policière le 22 septembre 2020 et celui du Collège des Procureurs Généraux le 7 janvier 2021.

II. INTRODUCTION

Pour exécuter leurs missions, les services de police utilisent de plus en plus les nouvelles technologies d'information et de communication.

Dans une société où une attention croissante est accordée à la sécurité des informations et à la protection des données à caractère personnel, les risques inévitablement liés aux traitements de ces informations et données par les services de police doivent être correctement encadrés et couverts en adoptant les mesures techniques et organisationnelles nécessaires.

La LFP prévoit que les ministres de la Justice et de l'Intérieur adoptent par le biais d'une directive contraignante les mesures nécessaires à cette fin. Pour déterminer ces mesures, nous nous sommes inspirés des " Baseline Information Security Guidelines " (BSG) du Centre pour la Cybersécurité Belgique. Nous souhaitons que ces lignes directrices constituent le cadre de référence pour la politique de sécurité de l'information et les plans de sécurité des services de police.

Les mesures contenues dans la présente directive visent à permettre aux services de police, qui ont des niveaux de maturité différents en matière de sécurité de l'information, d'augmenter leur niveau au fur et à mesure en utilisant la méthode éprouvée du PDCA (Plan-Do-Check-Act) et de renforcer la gestion des risques qui y est associée, d'assurer la continuité des activités policières, de prévenir la fuite d'informations, d'assurer la sécurité de son personnel et des citoyens et de renforcer ainsi la confiance de la société à leur égard.

Cette progressivité permet également de maintenir la continuité des activités policières opérationnelles tenant compte des moyens disponibles.

La présente directive définit les mesures minimales que les services de police doivent respecter lors de l'élaboration, l'implémentation et l'évaluation de la politique de sécurité de l'information, ainsi que les plans de sécurité et les procédures et processus qui concrétiseront la présente directive.

La mise en oeuvre progressive de la présente directive, ainsi que la définition des priorités, seront reprises dans la politique de sécurité de l'information, dans les plans de sécurité (voir ci-dessous), dans des notes internes à la police intégrée et/ou moyennant une mise à jour des fiches de la directive du 14 juin 2002 des Ministres de la Justice et de l'Intérieur (MFO-3) relative à la gestion de l'information de police judiciaire et de police administrative, lesquelles sont destinées aux services opérationnels.

Les chefs de corps pour la police locale et le commissaire général, les directeurs généraux et les directeurs pour la police fédérale sont les garants de la bonne exécution de ces directives en ce qui concerne les banques de données visées à l'article 44/2, §§ 1er et 3 LFP. Le cas échéant, une concertation entre les acteurs compétents en particulier le commissaire général, les directeurs généraux, les directeurs, les chefs de corps, le gestionnaire fonctionnel et le délégué à la protection des données compétent est fortement recommandée.

III. LES MESURES MINIMALES DE PROTECTION

1) La politique de sécurité de l'information et les plans de sécurité

Les services de police doivent disposer d'une politique actualisée et uniforme en matière de sécurité de l'information, ci-après " la politique de sécurité de l'information ", validée par le " comité de coordination de la police intégrée " (ci-après le CCGPI) après avis du " comité information et ICT " ³.

En tenant compte de la politique de sécurité de l'information, des plans de sécurité sont ensuite établis, qui contiennent les mesures techniques et organisationnelles de sécurité de l'information à mettre en oeuvre. Ces plans de sécurité, ainsi que les procédures et processus qui concrétiseront la présente directive, sont validés par la hiérarchie compétente, à savoir le Comité de direction pour la police fédérale et le Chef de Corps pour les zones de police, après avis du délégué à la protection des données compétent.

La politique de sécurité de l'information et les plans de sécurité, ainsi que les procédures et les processus qui concrétiseront la présente directive, doivent être évalués régulièrement.

Conformément à l'article 244 LPD, les services de police transmettent à l'Organe de contrôle de l'information policière (ci-après le " COC ") la politique en matière de sécurité de l'information ainsi que les plans de sécurité.

2) Organisation de la sécurité de l'information

Les services de police prévoient un système de gestion des risques en matière de sécurité de l'information et identifient les rôles et responsabilités des différents acteurs concernés par la sécurité de l'information.

Le délégué à la protection des données compétent est également chargé du suivi de la politique de sécurité des informations et de l'implémentation du(des) plan(s) de sécurité.

Afin de s'assurer que toutes les mesures organisationnelles soient appliquées, les services de police informent leur personnel et les tiers opérant sous leur responsabilité. La politique de sécurité et les plans de sécurité devront être disponibles et consultables par les personnes devant les appliquer. L'accès à toute l'information n'est néanmoins pas nécessaire pour atteindre cet objectif.

Les services de police développent, approuvent et communiquent des procédures et des bonnes pratiques pour la sécurité de l'information qui concrétiseront la présente directive.

Des procédures sont établies pour chaque utilisateur et en particulier pour ceux qui ont accès à des données avec une sensibilité particulière ou à des systèmes critiques.

Ces procédures portent sur les thèmes suivants :

- le contrôle d'accès / la gestion des autorisations ;
- le retrait des droits ;