

Privacyverklaring IG

-

Déclaration du Respect de la Vie Privée d'IG

[Versie N](#) / [Version F](#)

PRIVACYVERKLARING VAN IG

Privacy Statement (verklaring persoonlijke levenssfeer) van het Inspectoraat-generaal (IG)

INLEIDING

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. De AVG wordt aangevuld en uitgevoerd door de Privacywet van 30 juli 2018 (*wet ter bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*).

Het doel van onderhavige privacyverklaring is duidelijk te stellen:

- Waarom en op en welke basis wij (IG) persoonsgegevens verwerken;
- Welke categorieën persoonsgegevens wij verwerken in de dossiers (in het kader van de operationele processen);
- Met wie wij de persoonsgegevens kunnen delen;
- Hoelang wij persoonsgegevens bijhouden evenals de maatregelen die wij nemen om uw rechten evenals een correct gebruik van de persoonsgegevens te garanderen;
- Hoe een medewerker van Defensie of een derde zijn rechten kan uitoefenen en wie hij hiertoe kan contacteren.

PERSOONSgegevens IN DE OPERATIONELE PROCESSEN VAN IG

De bevoegdheden van IG worden opgenomen en zijn toegewezen krachtens het Reg A16-O1 (KB tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en tot vastlegging van de bevoegdheden van bepaalde autoriteiten van 02 december 2018).

Het bevoegde personeel van IG kan persoonsgegevens verwerken (ontvangen, opvragen, verzamelen, verifiëren, behandelen, verbeteren, vervolledigen, vernietigen, delen en/of bewaren) binnen de volgende operationele processen: onderzoek, evaluatie, klachten- en interventiebehandeling, coaching- en vormingsopdrachten (in het kader van ICS¹) en in de hoedanigheid van meldingspunt voor mogelijke integriteitsschendingen (integriteitscoördinator).

1. Waarom & op welke basis de persoonsgegevens worden verwerkt

- a. De vormen van onderzoek en de evaluaties die door IG kunnen uitgevoerd worden, verlopen altijd volgens een precies mandaat ingediend door een bevoegde autoriteit en gevalideerd door IG. Voor wat betreft de onderzoeken wordt een mandaat altijd uitgevaardigd door de Minister van Landsverdediging, CHOD² of IG zelf.
Sommige onderzoeken of evaluaties vereisen conform hun mandaat een verwerking van persoonsgegevens maar enkel indien dit noodzakelijk blijkt voor:
 - Het opmaken van een correcte en volledige output,
 - En, in voorkomend geval voor het formuleren van gerelateerde aanbevelingen.IG onderscheidt duidelijk zijn onderzoeksactiviteiten van deze van andere diensten met eigen (wettelijk) voorziene onderzoeksbevoegdheden: gerechtelijke onderzoeken, disciplinaire procedures, milieu-inspecties, etc. Het werkdomein van IG is functionering van Defensie.
- b. IG is wettelijk gehouden een antwoord te bieden op alle klachten of interventies die aan de dienst geadresseerd zijn,
 - Eerst over de ontvankelijkheid van de vraag,
 - Daarna, indien een vraag ontvankelijk is, over de grond ervan.

¹ Intern beheerssysteem

² Chef van Defensie

Met dit doel kan of moet IG bepaalde persoonsgegevens verwerken, en indien nodig, tevens in de te leveren antwoorden.

IG depersonaliseert de dossiers van het (globale) klachten- en interventiebeheer. Het betreft meer bepaald de opmaak van statistieken, van gerelateerde aanbevelingen of van adviezen. In geval van dwingende redenen zijn uitzonderingen toegelaten voor zover ze uitdrukkelijk gemotiveerd zijn.

IG kan een (vrijblijvende) tevredenheidsenquête organiseren met als enig doel de eigen werking van klachten- en interventiebeheer te verbeteren. Een deelnemer die wenst deel te nemen aan de enquête, zal hiertoe gevraagd worden het door IG toegewezen contact- of klachtendossiernummer kenbaar te maken en in te vullen. De resultaten van de enquête worden eveneens volledig gedepersonaliseerd.

- c. In zijn hoedanigheid van meldpunt voor eventuele schendingen van de integriteit (integriteitcoördinator), in samenwerking met de Federale Ombudsman en/of met de diensten van MOD of CHOD/Government Support kan het personeel van IG bepaalde persoonsgegevens verwerken:
 - Het ziet persoonsgegevens deze die voorkomen in de meldingen.
 - Het verifieert in geval van twijfel de juistheid ervan en/of laat ze vervolledigen.
 - Het kan bepaalde gegevens verwerken in de uitvoering van coördinerende activiteiten.
- d. IG is bevoegd om coachings- en vormingsopdrachten te geven in het kader van ICS. Het objectief van de coaching of vorming is op voorhand vastgelegd en ter kennis gebracht van een (de) stagiair(s). In deze context kan of moet IG, naargelang het geval, de individuele opvolging en/of beoordeling van de stagiairs maken en de resultaten ervan overmaken aan de bevoegde HR-diensten binnen Defensie.
- e. [†] IG ontvangt veel elementen van persoonsgebonden (gevoelige) informatie, ook ongevraagd. Deze kunnen echter een essentieel deel uitmaken van de context en de beoordeling van het geheel van een dossier van uit menselijk oogpunt.
- f. [†] In principe worden geen persoonsgegevens verwerkt in het kader van activiteiten van synthese (besluiten uit de activiteiten van IG) en bijstand door IG aan audits in de schoot van Defensie.

2. De categorieën persoonsgegevens wij verwerken in de dossiers in het kader van de operationele processen

Verskillende categorieën:

a. Zeer regelmatig: identificatiegegevens

- (1) Persoonlijke (elektronische) identificatiegegevens: naam, voornaam, beroep, titel, adres, vroegere adressen, telefoonnummer (werk, privé, fax), emailadres, identificatiegegevens toegekend door overheidsdiensten (stamnummer, ID-nummer, toegangskarten, ID-foto's...);
- (2) Identificatiegegevens uitgegeven door de overheidsdiensten: rijksregisternummer, identiteitskaartnummer, paspoortnummer, rijbewijsnummer, pensioennummer, nummerplaat.

b. Regelmatig: persoonlijke kenmerken:

- (1) Persoonlijke bijzonderheden: leeftijd, geslacht, geboortedatum, geboorteplaats, burgerlijke staat, nationaliteit;
- (2) Statutaire situatie: militair statuut, militair loopbaanoverzicht, militaire onderscheidingen, AGR overzichten (administratieve gegevens met uitsluiting van gegevens die vallen onder de voorschriften van medische geheimhouding).

c. Occasioneel: maatschappelijke gegevens:

- (1) Samenstelling van het gezin: gegevens betreffende huwelijk of huidige vorm van samenleven, vorige huwelijken of verbintenissen, (echt)scheidingen, vroegere partners, bijzonderheden betreffende andere familie- of gezinsleden;
- (2) Elementen betreffende reizen en verplaatsingen;

(3) Klachten, betrokkenheid bij incidenten of ongevallen: inlichtingen betreffende een ongeval, incident of klacht waarin de persoon die in het bestand is opgenomen betrokken is, aard van de schade of kwetsuren, betrokken personen, getuigen.

(4) Sociale media

d. Uitzonderlijk: opleiding, vorming, beroep:

(1) Academisch en schools curriculum: scholen, studies, gevolgde cursussen, diploma's, resultaten;

(2) Beroepsbekwaamheden: opleidingen, getuigschriften, licenties;

(3) Professionele ervaringen: interesses, specialisaties, vroegere ervaringen;

(4) Bijzonderheden inzake vorige betrekkingen en huidig beroep.

e. Zeer uitzonderlijk: financiële, juridische of gevoelige gegevens en beeldmateriaal

(1) Financiële bijzonderheden: loonfiches, prestatie fiches, gegevens betreffende sociale en familiale vergoedingen, nummers van bankrekeningen;

(2) Gerechtelijke gegevens: PV's opgesteld door de politiediensten, PV's van gerechtelijke gehoorverslagen en arresten, etc....;

(3) Eventuele ter beschikking gestelde beeld- en/of geluidsopname, heel sporadisch en alleen indien het echt nodig is voor de afwerking van een dossier.

(4) Gevoelige informatie: gegevens die te maken hebben met raciale of etnische achtergrond, politieke opinies, godsdienstige of filosofische overtuigingen, vakbondslidmaatschap, seksuele geaardheid.

f. Opmerking - medische gegevens

IG vraagt geen inzage in gegevens die vallen onder de bescherming van het medisch geheim (enkel administratieve gegevens indien nodig zoals afwezigheden voor medische redenen, data van hospitalisaties, etc.). Toch gebeurt het, in het bijzonder voor het gedeelte klacht- en interventie behandeling, dat medische gegevens spontaan aan personeel van IG ter beschikking worden gesteld en er acte van genomen wordt. Inderdaad kan een betrokkene van mening zijn dat bepaalde medische feitelijkheden moeten gekend zijn door IG ten einde een situatie beter te begrijpen of te beoordelen met het oog op een juiste output. IG kan, indien nodig, deze gegevens bekijken van uit menselijk oogpunt om de coherentie van het geheel beter te garanderen. Niettemin zal het deze nooit (mogen) uitbaten op een manier die in tegenstrijd zou kunnen zijn met de wetgeving op de uitoefening van de medische beroepen, een wetgeving van openbare orde.

g. Opmerking - derden - gegevensbanken

(1) Informatie die gerelateerd is aan een dossier kan ook persoonsgegevens bevatten van andere fysieke personen (derden), echter alleen indien deze onontbeerlijk zijn voor de juiste beoordeling, de relevantie of de begrijpbaarheid van een output.

(2) Bovenstaande lijst is niet exhaustief. Persoonsgegevens die worden bijgehouden en verwerkt binnen het contact- en klachtenmanagement, zijn opgenomen in het register van gegevensverwerking (GDPR register IG - gerarchiveerde databank BODI¹ - actuele databank DLex²) dat ten alle tijde kan worden geraadpleegd.

3. Met wie de persoonsgegevens worden gedeeld

a. Binnen de Europese Economische Ruimte (EER)

Om de hogervermelde opdrachten te vervullen, kan het daartoe bevoegd personeel persoonsgegevens delen:

(1) Met alle bevoegde medewerkers van IG belast met de behandeling en opvolging van activiteiten in de genoemde processen;

¹ Archiveringsstelsel beheer klachten en contacten vóór 2019

² Archiveringsstelsel beheer klachten en contacten na 2019

- (2) In voorkomend geval in het kader van multidisciplinaire dossiers, met medewerkers van Defensie, meestal van MOD, CHOD, DG BudFin¹, DG Jur², DG H&W³ of DGHR⁴ voor actie of Info binnen de hun toegewezen bevoegdheidsdomein.
- (3) Voor zover de privacy wet het toelaat of oplegt, met publieke en gerechtelijke autoriteiten of instanties op hun vraag of op ons initiatief, in het bijzonder met de Federale Ombudsman, het (Federale) Parlement of parlementaire commissies en politie- en gerechtelijke diensten.

Het betreft onze meest voorkomende gesprekspartners.

Het delen van gegevens kan in twee richtingen.

b. Buiten de Europese Economische Ruimte (EER)

- (1) *"De doorgifte van deze gegevens naar een land buiten de EER of een internationale organisatie zal slechts uitgevoerd worden als door de Europese Commissie wordt erkend dat deze een passend niveau van bescherming van persoonsgegevens garanderen."*⁵
- (2) *"Als, in afwijking van dit principe, deze gegevens toch moeten doorgegeven worden naar landen buiten de EER en internationale organisaties waarvan door de Europese Commissie niet erkend is dat zij een passend niveau van bescherming van persoonsgegevens waarborgen, zullen wij het nodige doen om passende waarborgen te bieden met het oog op de bescherming van uw rechten en belangen in dit land."*⁶
- (3) IG heeft (voorlopig) geen toepassingsdomein voor het afsluiten van protocollen in uitvoering van Art 20 van de wet handelend over verwerking van persoonsgegevens van 30 juli 2018 (zie inleiding).

4. Hoelang de persoonsgegevens worden bijgehouden

Uw persoonsgegevens worden bewaard zolang vereist is om te voldoen aan de toepasselijke (archivering) regels met in acht neming van de nationale historische waarde en/of zolang als nodig voor het afsluiten van een dossier.

BEVEILIGING: DE MAATREGELEN DIE WORDEN GENOMEN OM UW RECHTEN EVENALS OM EEN CORRECT GEBRUIK VAN DE PERSOONSgegevens TE GARANDEREN

IG treft passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, waaronder, bovenop de toepassing van de regelgeving terzake, in het bijzonder:

1. Het personeel van IG wordt regelmatig herinnerd aan de richtlijnen en reglementering met betrekking tot de bescherming van persoonsgegevens. Ook nieuwe medewerkers moeten uitvoerig gebriefd worden over deze materie.
2. De waarde "respect" is essentieel voor de activiteiten van IG. Ze is opgenomen in de deontologische code en uitdrukkelijk gepubliceerd op de SHP⁷. Elk jaar voorziet IG voor zijn personeel een heropfrissingsmoment van die code in hoofde van al zijn personeel.
3. In de context van het integriteitsbeleid stelt IG zich op als een referentie en een feitelijke bewaker van het correct gebruik van persoonsgegevens.

¹ Algemene Directie Budget en Financiën

² Algemene Directie Juridische Steun

³ Algemene Directie Health en Wellbeing

⁴ Algemene Directie Human Resources

⁵ Bronvermelding Privacy Statement Algemene Directie Juridische Steun (DGJur)

⁶ Idem

⁷ Sharepoint

4. Er bestaat een centraal entry point binnen IG (integriteitscoördinator) voor de transit van alle correspondentie met betrekking tot coördinatieactiviteiten ter zake.
5. Elk gevoelig onderzoek en elke evaluatie wordt voorafgegaan door een risicoanalyse waaronder deze met betrekking tot de verwerking van persoonsgegevens in het bijzonder de gevoelige informatie.
6. De dossiers van de verschillende operationele processen, behoudens een aantal routinetaken, wordt geëchelonneerd gecontroleerd.
7. Van complexe dossiers wordt een agenda of een soort "logboek" bijgehouden met de gerelateerde activiteiten waaronder de verwerking van persoonsgegevens.
8. IG beraadt zich systematisch bij DJMM¹ alvorens delicate informatie met gerechtelijke instanties of politie te delen.
9. De toegangsrechten tot dragers (applicaties) van persoonsgebonden gegevens worden centraal beheerd.
10. De parameters voor gebruik van de databank BODI voor klachtenbehandeling worden in het GDPR-register van Defensie opgenomen.
11. Voor gevoelige dossiers gebruikt IG gepersonaliseerde mailboxen (en geen collectieve mailboxen).
12. De parameters voor archivering en archiveringsduur zijn bepaald per type informatie en per recordsysteem.
13. IG vernietigt stukken die persoonsgegeven bevatten wanneer deze niet meer nodig zijn voor de verwerking van een dossier en houdt een spoor bij van die activiteit (in het bijzonder informatie uit het nationaal register). Indien mogelijk worden bepaalde persoonsgegevens onzichtbaar gemaakt (in het bijzonder gegevens die vallen onder de bescherming van het medisch geheim). Er kunnen intern periodieke controles en steekproeven worden uitgevoerd.
14. Het personeel van IG kan met vragen terecht bij de POC², de infomanager van IG, die ze beantwoordt of voorlegt aan de experts van DGJur.

WAT ZIJN UW RECHTEN

1. Rechten

"In overeenstemming met de toepasselijke regelgeving hebt u het recht op:

- *Inzage: u kan informatie krijgen over de verwerking van uw persoonsgegevens en een kopie ervan bekomen.*
- *Rectificatie: als u meent dat uw persoonsgegevens onjuist of onvolledig zijn, kan u vragen dat deze persoonsgegevens worden aangepast.*
- *Wissing: u kan in bepaalde omstandigheden vragen uw persoonsgegevens te wissen.*
- *Beperking: u kan de beperking van de verwerking van uw persoonsgegevens vragen indien deze inaccuraat zijn, onrechtmatig bekomen, niet langer nodig zijn of een gerechtvaardigde reden van bezwaar heeft.*
- *Bezwaar: u kan bezwaar maken tegen de verwerking van uw persoonsgegevens om redenen die verband houden met uw specifieke situatie.*
- *Intrekking van uw toestemming: indien u uw toestemming hebt gegeven voor het verwerken van uw persoonsgegevens, hebt u steeds het recht om deze toestemming in te trekken.*
- *Gegevensoverdraagbaarheid: voor zover wettelijk van toepassing, hebt u het recht om de persoonsgegevens die u aan ons hebt verstrekt te verkrijgen of, voor zover technisch mogelijk, over te dragen aan een derde partij."*³

¹ Gerechtelijke Politie in Militair Milieu

² Point Of Contact

³ Bronverwerking DGJur

2. Contacten

- a. Voor de uitoefening van rechten: indien men één van voornoemde rechten wenst uit te oefenen, kan men de DPO¹ via het volgend emailadres contacteren: dpo@mil.be.
- b. In overeenstemming met de toepasselijke regelgeving heeft men, naast de hierboven vermelde rechten, het recht om een klacht in te dienen bij de bevoegde toezichthoudende autoriteit, zijnde de Belgische gegevensbeschermingsautoriteit: www.gegevensbeschermingsautoriteit.be.
- c. Indien u vragen, opmerkingen of klachten zou hebben betreffende dit beleid en hoe IG uw persoonsgegevens verwerkt of indien er aanwijzingen zijn van misbruik, neem dan contact op via e-mail IG: IG-SRT@mil.be of het contactformulier op de intranetsite DG Jur of via email dpo@mil.be.

¹ Data protection Officer

DECLARATION DU RESPECT DE LA VIE PRIVEE D'IG

Privacy statement (déclaration de confidentialité) de l'Inspection Générale (IG)

INTRODUCTION

Depuis le 25 mai 2018, le Règlement général pour la protection des données (RGPD) est entré en vigueur. Ce RGPD est complété et exécuté par la [Loi sur la vie privée](#) du 30 juillet 2018 (loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel).

L'objectif de la présente déclaration de confidentialité est d'indiquer :

- Dans quel but et sur quelle base nous (l'IG) traitons des données à caractère personnel ;
- Les catégories de données à caractère personnel que nous exploitons dans les dossiers de nos processus opérationnels ;
- Avec qui nous partageons les données à caractère personnel ;
- La durée de conservation des données à caractère personnel ainsi que les mesures prises afin de les exploiter correctement et de garantir vos droits ;
- De quelle façon le personnel de la Défense ainsi que de tierces personnes peuvent exercer leurs droits et qui contacter au besoin.

DES DONNEES A CARACTERE PERSONNEL DANS LES PROCESSUS OPERATIONNELS DE L'IG

Les compétences d'IG sont stipulées et attribuées par le Rég A16-O1 (AR déterminant la structure générale du Ministère de la Défense et fixant les attributions de certaines autorités du 24 janvier 2019). Le personnel compétent d'IG est autorisé à traiter des données à caractère personnel (demander, collecter, vérifier, utiliser, corriger, compléter, détruire, partager et/ou conserver) en dedans les processus opérationnels suivants: l'enquête, l'évaluation, le traitement et la gestion des plaintes et des interventions, le coaching et les tâches de formation (dans le cadre ICS¹) et dans sa capacité de point de signalement dans le cas d'une possible atteinte à l'intégrité (coordinateur d'intégrité)

1. Dans quel but et sur quelle base nous traitons des données à caractère personnel

- a. Les types d'enquêtes et les évaluations pouvant être effectuées par l'IG sont toujours exécutées selon un mandat précis introduit par une autorité compétente et validé par IG. En ce qui concerne les enquêtes un mandat est toujours promulgué par le Ministre de la Défense, CHOD² ou l'IG même. Certaines enquêtes ou évaluations exigent, conformément à leur mandat le traitement des données à caractère personnel, mais uniquement si cela s'avère indispensable :
 - En vue de rédiger un dossier correct et complet,
 - Et, le cas échéant en vue de formuler des recommandations relatives.L'IG fait clairement la distinction entre ses propres activités et celles des autres instances avec leurs propres compétences de recherche (légalement) prévues : enquêtes judiciaires, procédures disciplinaires, inspections environnementales, etc.) Son domaine de travail se limite au fonctionnement de la Défense.
- b. L'IG est tenu légalement de répondre à toutes les plaintes et interventions qui lui sont adressées,
 - D'abord sur la recevabilité
 - Ensuite, si une question est recevable, sur son fond.

¹ Système de Contrôle Interne

² Chef de la Défense

A cette fin l'IG peut ou doit traiter des données à caractère personnel, si nécessaire, également dans les réponses à fournir.

L'IG dépersonnalise tous les dossiers du processus de gestion (globale) des plaintes et/ou des interventions. Il s'agit notamment de la rédaction de statistiques, de recommandations relatives ou d'avis. Pour des raisons contraignantes les exceptions sont autorisées pour autant qu'elles soient motivées explicitement.

IG peut organiser (sans engagement) une enquête de satisfaction qui a pour unique but d'améliorer son propre fonctionnement de la gestion des plaintes et des interventions. Chaque participant qui désire répondre à une enquête devra introduire son numéro de dossier. Les résultats de cette enquête seront entièrement dépersonnalisés.

- c. Dans sa capacité de point de signalement d'une éventuelle atteinte à l'intégrité en coopération avec le Médiateur Fédéral et/ou les services du MOD ou CHOD/Gouvernement Support, le personnel de l'IG traite des données à caractère personnel :
 - Il voit les données qui figurent dans les signalements.
 - Il vérifie en cas de doute si les données sont correctes ou non et/ou les fait compléter.
 - Il peut traiter certaines données lors de ses activités de coordination.
- d. L'IG est habilitée à faire du coaching et à donner des formations dans le cadre ICS. L'objectif d'un coaching ou d'une formation sont préalablement définis et communiqués pour prise de connaissance aux stagiaire(s) concerné(s). Dans ce contexte, l'IG peut ou doit selon le cas, faire un suivi et/ou une évaluation individualisée de ses stagiaires et transmettre les résultats aux services compétents de RH au sein de la Défense.
- e. † L'IG reçoit beaucoup d'éléments d'information à caractère personnel (sensibles), dont certains non demandés. Ils peuvent constituer une partie essentielle d'un contexte et d'une appréciation de l'entièreté d'un dossier d'un point de vue humain.
- f. † En principe nous ne traitons pas de données à caractère personnel dans le cadre d'activités de synthèse (conclusions des activités d'IG) et de l'assistance par l'IG aux audits au sein de la Défense.

2. Les catégories de données à caractère personnel que nous exploitons dans les dossiers de nos processus opérationnels

Différentes catégories

a. Très régulièrement : données d'identification

- (2) Données d'identification personnelles et/ou électroniques : nom, prénom, profession, titre, adresse, anciennes adresses, numéro de téléphone (travail, privé, fax), adresse e-mail (travail, privée), données d'identification attribuées par les services publics (N° immatriculation, N° ID, photo-ID, ...):
- (3) Données d'identification émises par les services publics : numéro de registre national, numéro de carte d'identité, numéro de passeport, numéro de permis de conduire, numéro de pension, plaque d'immatriculation.

b. Régulièrement : caractéristiques personnelles

- (1) Détails personnels : âge, sexe, date de naissance, lieu de naissance, état civil, nationalité ;
- (2) Situation militaire : statut, parcours, distinctions, récapitulatifs AGR (données administratives avec exclusion de données qui sont soumises aux directives du secret médical).

c. Occasionnellement: données sociales

- (1) Composition du ménage : données relatives au mariage ou à la forme actuelle de cohabitation, unions ou mariages précédents, divorces, séparations, partenaires précédents, détails sur les autres membres de la famille ou du ménage ;
- (2) Détails relatifs aux voyages et déplacements ;

- (3) Plaintes, incidents ou accidents : informations relatives à un accident, un incident ou une plainte impliquant la personne fichée, nature des dommages ou blessures, personnes impliquées, témoins ;
- (4) Médias sociaux.
- d. Exceptionnellement : études, formation, profession
 - (1) Curricula académiques : écoles, études, cours suivis, diplômes, résultats ;
 - (2) Qualifications professionnelles : formations, brevets, licences ;
 - (3) Expériences professionnelles : intérêts, spécialisations, expériences passées ;
 - (4) Détails relatifs aux emplois précédents et à l'emploi actuel..
- e. Très exceptionnellement : détails financiers, détails judiciaires, des enregistrements d'images et/ou de sons et informations délicates
 - (1) Détails financiers : des fiches salariales, des fiches prestataires, des données relatives aux allocations familiales et sociales et numéros d'identification et de compte en banque ;
 - (2) Détails judiciaires : PV rédigés par les agents de police, PV des auditions judiciaires et des arrêts, etc ;
 - (3) Des enregistrements d'images et/ou de sons sont sporadiquement utilisés et uniquement s'ils sont nécessaires au traitement d'un dossier.
 - (4) Informations délicates : données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle.
- f. ⚠ Remarque - Données médicales

IG ne demande pas d'avoir une vue sur des données qui sont protégées par le secret médical (uniquement, si nécessaire, sur des données administratives telles que des absences pour raison de santé, des dates d'une hospitalisation, etc). Cependant il arrive, en particulier lors de l'introduction d'une plainte ou d'une intervention, que des données médicales soient spontanément mises à disposition du personnel d'IG et qu'on en prenne acte. En effet, il se peut qu'un intéressé estime que l'IG ait besoin de connaître certains faits médicaux afin de mieux comprendre ou apprécier une situation en vue d'un output correct. L'IG pourra dès lors analyser ses données d'un point de vue humain afin de garantir une meilleure cohérence de l'ensemble. Toutefois, l'IG n'exploite jamais (et ne peut le faire) ces données de sorte à ne pas être en opposition avec la législation relative à la pratique des professions médicales, ou toute autre législation d'ordre public.
- g. ⚠ Remarque - tiers - banque de données
 - (1) Les informations relatives au dossier peuvent contenir des données à caractère personnel d'autres personnes physiques, pour autant qu'elles soient indispensables au traitement et/ou à la bonne compréhension d'un dossier.
 - (2) Cette liste n'est pas exhaustive. Toutes les données à caractère personnel conservées et traitées dans le cadre de la gestion des plaintes sont reprises dans le registre du traitement de données et peuvent être consultées à tout moment (GDPR registre IG - banque d'archivage : BODI¹ - banque de données actuelles : DLex²).

3. Avec qui nous partageons les données à caractère personnel

a. En dedans l'Espace économique européen (EEE)

En vue d'atteindre les objectifs visés stipulés ci-dessus, le personnel compétent d'IG les partage :

- (1) Avec des collaborateurs d'IG chargés du traitement et du suivi des dossiers et activités desdits processus.

¹ Système d'archivage de dossiers de plaintes avant 2019

² Base de données et de gestion de plaintes à partir de 2019

- (2) Dans le contexte des dossiers multidisciplinaires, avec des collaborateurs au sein de la Défense, le plus souvent du MOD, CHOD, de la DG BF¹, DG Jur², DG H&WB³ ou de la DG HR⁴ pour action ou pour Info en dedans leurs compétences attribuées.
- (3) Pour autant que la loi sur la confidentialité l'autorise ou l'impose avec des autorités ou instances publiques ou judiciaires, sur leur demande ou sur notre initiative, en particulier avec le Médiateur Fédéral, le Parlement (Fédéral) ou les commissions parlementaires et les services de police ou judiciaires.

Il s'agit de nos interlocuteurs les plus courants.

Le partage de données se fait dans les deux sens.

b. En dehors l'Espace économique européen (EEE)

- (1) « En dehors l'Espace économique européen (EEE) la transmission de ces données vers un pays extérieur à l'EEE (Espace économique européen) ou une organisation internationale ne sera effectuée que si ceux-ci sont reconnus par la Commission européenne comme garantissant un niveau approprié de protection des données à caractère personnel. »⁵
- (2) « Si, par dérogation à ce principe, ces données devaient quand même être transmises vers des pays extérieurs à l'EEE et organisations internationales non reconnus par la Commission européenne comme garantissant un niveau approprié de protection des données à caractère personnel, nous veillerons à ce que soit garantie de manière adéquate la protection de vos droits et intérêts dans le pays de destination. »⁶
- (3) IG n'a (provisoirement) aucun domaine d'explication pour conclure des protocoles en conformité avec l'Art 20 de la loi sur les données à caractère personnelles du 30 juillet 2018 (voir introduction).

4. Combien de temps nous conservons les données à caractère personnel ?

Vos données à caractère personnel seront conservées tant que la réglementation (d'archivage) en vigueur l'impose tout en considérant la valeur nationale d'archivage ou pour la durée nécessaire à clôturer un dossier.

PROTECTION : LES MESURES QUE NOUS PRENONS AFIN DE GARANTIR UN TRAITEMENT CORRECT DES DONNEES A CARACTERE PERSONNEL

IG met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques éventuels.

1. Le personnel d'IG est régulièrement briefé quant aux directives et à la réglementation sur la confidentialité des données à caractère personnel. Les nouveaux collaborateurs en sont briefés consciencieusement.
2. La valeur du « respect » est essentielle pour les activités de l'IG. Elle est reprise dans son code déontologique et explicitement publiée sur son SHP⁷. Chaque année l'IG organise remise à niveau de tout son personnel.

¹ Direction Générale Budgets&Finances

² Direction Générale Appui Juridique

³ Direction Générale Health&Wellbeing (Bien être au travail)

⁴ Direction Générale Human Resources (Ressources humaines)

⁵ Source Déclaration Protection des Données de la Direction Général Appui Juridique

⁶ IDEM

⁷ Sharepoint

3. Dans le contexte de la politique sur l'intégrité, IG se profile de fait comme une référence et un gardien de l'utilisation correcte de données à caractère personnel.
4. Il existe UN point d'entrée chez IG (coordinateur intégrité) par lequel transite tout le courriel relatif aux activités de coordination en question.
5. Chaque enquête et chaque évaluation effectuée par IG est précédée d'une analyse de risque en incluant celle sur le traitement éventuel de données à caractère personnel et en particulier en ce qui concerne des données dites sensibles dans le domaine de la vie privée.
6. Tous les dossiers des processus opérationnels sont soumis à un contrôle échelonné sauf quelques activités administratives récurrentes.
7. Pour les dossier complexes l'IG tiendra un agenda ou un genre de « logboek » où sont notées toutes les activités relatives, y compris le traitement de données à caractère personnel.
8. L'IG demande un avis de DJMM¹ avant de partager des informations délicates avec les instances judiciaires ou avec la police.
9. L'IG mène une gestion centralisée quant aux accès aux différents porteurs (applications) de données.
10. IG a repris les paramètres d'utilisation de la banque de données BODI et DLex pour le traitement et la gestion des plaintes dans le registre RGPD.
11. Pour certains dossiers délicats, l'IG n'utilise que des mail box personnalisées (et non collectives).
12. Les paramètres d'archivage et la durée d'archivage sont déterminés par type d'Info et par système d'archivage.
13. IG détruit les pièces qui contiennent des données à caractère personnel après traitement tout en conservant une trace de cette activité. Si c'est possible certaines données sont rendues invisibles (en particulier des données protégées par le secret médical). Il y a possibilité de faire des contrôles périodiques et des vérifications ponctuelles.
14. Le personnel d'IG peut s'adresser à un POC², le gestionnaire d'information de l'IG, qui répond aux questions ou les soumet aux experts de DGJur.

DE QUELLE FAÇON LE PERSONNEL DE LA DEFENSE AINSI QUE DE TIERSES PERSONNES PEUVENT EXERCER LEURS DROITS ET QUI CONTACTER AU BESOIN ?

1. Vos droits

« Conformément à la réglementation applicable, vous disposez des droits suivants :

- *Droit d'accès : vous pouvez obtenir des informations sur le traitement de vos données à caractère personnel ainsi qu'une copie de celles-ci.*
- *Droit de rectification : si vous estimez que vos données à caractère personnel sont inexactes ou incomplètes, vous pouvez demander leur adaptation.*
- *Droit à l'effacement : dans certaines circonstances, vous pouvez demander l'effacement de vos données à caractère personnel.*
- *Droit à la limitation du traitement : vous pouvez demander la limitation du traitement de vos données à caractère personnel si celles-ci sont inexactes, ont été obtenues illicitement, ne sont plus utiles ou si vous avez une raison légitime de vous y opposer.*
- *Droit d'opposition : vous pouvez vous opposer au traitement de vos données à caractère personnel pour des raisons liées à votre situation particulière.*

¹ Police Judiciaire Milieu Militaire

² Point de Contact

- *Droit au retrait de votre consentement : si vous avez donné votre consentement pour le traitement de vos données à caractère personnel, vous avez le droit de retirer ce consentement à tout moment.*
- *Droit à la portabilité de vos données : quand ce doit est applicable, vous avez le droit de recevoir les données à caractère personnel que vous nous avez fournies ou, lorsque cela est techniquement possible, de les transférer à un tiers. »¹*

2. **Contacts**

- a. Si vous souhaitez exercer l'un des droits susmentionnés, vous pouvez contacter le DPO² à l'adresse e-mail suivante : dpo@mil.be .
- b. « Conformément à la réglementation en vigueur, vous disposez, outre les droits susmentionnés, du droit d'introduire une plainte auprès de l'autorité de contrôle compétente, à savoir l'Autorité belge de protection des données www.autoriteprotectiondonnees.be » (Référence de la source Privacy Statement DGJur)
- c. Si vous avez des remarques, des questions ou des plaintes sur cette déclaration ou sur la façon dont IG traite vos données à caractères personnel ou si vous constatez des indices d'abus, vous pouvez prendre contact via l' e-mail de l'IG: IG-SRT@mil.be ou par le formulaire de contact sur le site intranet de DGJur ou par e-mail dpo@mil.be

¹ Source Déclaration Protection des Données de la Direction Général Appui Juridique

² Officier de protection des données