Lignes directrices concernant l'application du Règlement du Conseil de l'Europe sur la protection des données dans le cadre des activités de la Direction de l'Audit interne, de l'Évaluation et de l'Investigation (DIO)

LIGNES DIRECTRICES SUR LA PROTECTION DES DONNÉES
DANS LE CADRE DES ACTIVITÉS DE LA DIO

Dispositions générales

Article 1

Objet et but

1.1 La protection des données à caractère personnel est un droit fondamental régi par la Convention européenne des droits de l'homme et par le Règlement du Conseil de l'Europe (CdE) sur la protection des données, qui se réfère aux principes de protection des données figurant dans la Convention 108 et ses protocoles d'amendement. Les présentes Lignes directrices ont pour but de guider les personnes qui mènent des évaluations, des missions d'assurance (audits), des missions de consultance et des processus d'investigation, ainsi que d'établir des garanties spécifiques de protection des données pour le traitement des données à caractère personnel effectué dans le cadre de ces activités. Ce traitement est susceptible d'interférer avec les droits et les libertés fondamentales des personnes prenant part aux activités concernées, en particulier le droit au respect de leur vie privée.

1.2 Les présentes Lignes directrices visent à compléter le Règlement du Conseil de l'Europe sur la protection des données à caractère personnel (le « Règlement ») et d'autres dispositions régissant les activités de la DIO relatives au traitement des données à caractère personnel et n'ont pas pour objet de les remplacer. Elles décrivent plutôt les besoins spécifiques de la DIO dans le domaine de la protection des données lorsqu'elle réalise des évaluations, des missions d'assurance (audits), des missions de consultance et des processus d'investigation.

1.3 Les présentes Lignes directrices ont pour but :

- de s'assurer que les règles de protection des données relatives à l'utilisation de différents moyens de collecte de preuves sont consignées par écrit et que les moyens les moins intrusifs sont utilisés pour la collecte de données à caractère personnel ;
- d'informer pleinement les personnes qui mènent des activités impliquant le traitement de données à caractère personnel des règles applicables au traitement d'informations sensibles ;
- d'aider les personnes qui mènent les activités décrites dans les présentes Lignes directrices à définir ce que sont les « données personnelles » dans ce contexte et qui sont les personnes concernées par le traitement et à déterminer leurs droits d'information, d'accès et de rectification. Il convient de tenir compte du fait que le Règlement autorise la restriction de ces droits, à condition que la nécessité et la proportionnalité d'une telle restriction soient évaluées, respectées et documentées ;
- de fournir des orientations sur la manière d'évaluer la compétence adéquate du destinataire des données (interne ou externe), puis de limiter le transfert d'informations à caractère personnel à ce qui est strictement pertinent et nécessaire ;
- de préciser comment mettre en œuvre des mesures de sécurité fondées sur une analyse d'évaluation des risques afin de garantir un traitement licite et sécurisé des données à caractère personnel.

Article 2

Définitions

Aux fins des présentes Lignes directrices :

2.1 Les définitions figurant à l'article 2 du Règlement du Conseil de l'Europe sur la protection des données à caractère personnel s'appliquent chaque fois que les termes concernés sont utilisés dans les présentes ;

2.2 Le terme « DIO » désigne la Direction de l'Audit interne, de l'Évaluation et de l'Investigation dans son ensemble, c'est-à-dire la division de l'Audit, la division de l'Évaluation et la division de l'Investigation ainsi que la division centrale chargée des tâches administratives générales ;

2.3 Le terme « évaluations » désigne les examens impartiaux et méthodiques d'activités, de projets, de programmes, de stratégies, de politiques, de sujets, de thèmes, de secteurs, de domaines opérationnels ou de performances institutionnelles, telles que définies par la Politique d'évaluation du Conseil de l'Europe ;

2.4 Le terme « missions d'assurance » désigne les audits consistant en une analyse objective d'éléments factuels aux fins d'examen indépendant de la performance, de la gouvernance, de la gestion des risques et des processus de contrôle de l'Organisation, dont la nature et le périmètre sont déterminés par la fonction d'Audit interne, telle que définie par la Charte de la DIO ;

2.5 Le terme « activités de consultance » désigne les activités de conseil et d'autres activités liées au service client, dont la nature et le périmètre sont convenus avec le management. Ces activités ont pour objectif d'apporter une valeur ajoutée et d'améliorer la gouvernance, la gestion des risques et les processus de contrôle de l'Organisation sans que la fonction d'Audit interne n'assume de responsabilité managériale, telle que définie par la Charte de la DIO ;

2.6 Le terme « processus/procédure d'investigation » désigne le processus visant à déterminer si un acte de fraude, de corruption ou un autre acte répréhensible, tel que défini par le cadre juridique de l'Organisation, a été commis ;

2.7 Le terme « personne faisant l'objet d'une investigation » désigne toute personne visée par une investigation relative à des allégations d'actes répréhensibles, tels que définis par le cadre juridique de l'Organisation.

Article 3

Portée

3.1 Les présentes Lignes directrices s'appliquent au traitement des données à caractère personnel effectué par la DIO dans l'exercice de toutes les activités relevant de son mandat, telles que les évaluations, les missions d'assurance (audits), les missions de consultance, les processus d'investigation et toutes les activités administratives et de soutien menées par sa division centrale. La DIO s'engage à respecter les principes de protection des données à caractère personnel énoncés à l'article 4 du Règlement du Conseil de l'Europe sur la protection des données à caractère personnel.

3.2 Les présentes Lignes directrices et les exemples qu'elles contiennent sont destinés à servir de guide pratique aux agents de la DIO chargés de mener les activités relevant de la compétence de leur Direction ; elles doivent donc être considérées comme indicatives par nature. Elles ne créent pas de droit substantiel ni ne confèrent, n'imposent ou n'impliquent de nouveaux droits ou obligations autres que ceux prévus dans le cadre juridique du CdE, pouvant être invoqués devant une instance judiciaire ou dans le cadre de procédures administratives menées par ou contre les agents du CdE ou de la DIO responsables de la conduite des activités concernées.

Article 4

Légitimité du traitement des données

4.1 Les activités menées par la DIO visent à protéger les intérêts du CdE, à fournir une assurance indépendante et objective à son management et à ses États membres et à l'aider à atteindre ses objectifs. La DIO peut être amenée à accéder à des données à caractère personnel et à les traiter afin de répondre au besoin légitime de mener les activités nécessaires à l'accomplissement de son mandat, tel que défini dans la Charte de la DIO et conformément au cadre juridique de l'Organisation.

4.2 La DIO examine toutefois, au cas par cas, si le traitement des données est nécessaire et proportionné.

4.3 La DIO veille à ce que tout traitement de données soit conforme au cadre de l'Organisation en matière de protection des données. Elle peut accéder aux données déjà détenues et traitées par l'Organisation, les demander, les obtenir et les traiter d'une autre manière, s'il existe un besoin légitime à cet égard, et dans le respect des principes susmentionnés de nécessité et de proportionnalité de ce traitement. Le cadre juridique de l'Organisation prévoit explicitement que la DIO peut avoir accès à toute information qu'elle juge nécessaire et proportionnée pour remplir son rôle.

4.4 La DIO s'engage également à respecter les principes généraux de licéité, de loyauté et de transparence, de limitation des finalités, de minimisation des données, d'exactitude et de sécurité.

Article 5

Traitements portant sur des catégories particulières de données

5.1 Compte tenu de la nature des activités et du mandat de la DIO, le traitement des données à caractère personnel, quel que soit le degré de sensibilité de ces données, est effectué avec des garanties complémentaires adéquates s'il intervient dans le cadre d'une évaluation, d'une mission d'assurance, d'une mission de consultance ou d'un processus d'investigation.

Article 6

Sécurité des données

6.1 La DIO s'engage notamment à prendre les mesures de sécurité suivantes contre des risques tels que l'accès accidentel ou non autorisé aux données à caractère personnel, leur destruction, leur perte, leur utilisation, leur modification ou leur divulgation non autorisée :

- politique de bureau propre : aucune information sensible ne doit être accessible sur le poste de travail en cas d'absence prolongée et, dans tous les cas, à la fin de la journée de travail, qu'il s'agisse de documents papier contenant des données à caractère personnel ou d'appareils non protégés tels que les ordinateurs portables et des clés USB ;
- politique de mise sous clé : des armoires et des tiroirs fermant à clé sont utilisés pour le stockage de documents et de dossiers en cas d'absence ; les bureaux sont fermés à clé en cas d'absence prolongée et, dans tous les cas, à la fin de la journée de travail ;
- utilisation exclusive du mode d'impression sécurisée pour tous les documents contenant des données à caractère personnel ;
- impression des documents contenant des données à caractère personnel réservée aux seuls cas de nécessité ;
- broyage des dossiers physiques à jeter ou application de mesures équivalentes pour éviter qu'ils puissent être récupérés ;
- pseudonymisation et cryptage des données à caractère personnel, dans la mesure du possible et lorsque nécessaire ;
- interdiction d'emporter des documents en dehors des locaux, sauf autorisation spéciale et/ou nécessité impérieuse liée au travail.

6.2 Outre ces engagements, la DIO met en œuvre les politiques applicables et s'efforce de suivre les lignes directrices et les bonnes pratiques formulées par la Direction des technologies de l'information (DIT), en particulier :

- politique de l'écran vide : l'écran de verrouillage est activé lorsque le poste de travail est laissé sans surveillance, même pour une courte durée ;
- consignes de sécurité opérationnelle applicables au télétravail : il s'agit notamment d'éviter de travailler sur des documents sensibles dans des espaces publics et via des réseaux publics, d'accéder à l'intranet uniquement à partir de dispositifs fiables et de réseaux privés, de veiller à éviter de télécharger inutilement des fichiers et, dans tous les cas, de supprimer les fichiers téléchargés dès que possible ;
- utilisation de groupes d'accès dans le Data Management System, géré en interne par la DIO.

6.3 Compte tenu de la nécessité d'assurer un niveau de sécurité adéquat pour certains types de documents et/ou d'informations, la fonction d'Investigation peut recourir à des mesures de sécurité complémentaires pour le stockage, telles que des coffres-forts situés dans les locaux de l'Organisation.

6.4 Au titre de l'obligation de notification des violations de données à la personne déléguée à la protection des données, chaque fois que la DIO détecte une violation de données, le directeur ou la directrice de la DIO en est immédiatement informé-e par écrit.

6.5 Sauf indication contraire, les agents de la DIO sont tenus de signaler les violations de données portées à son attention, en utilisant le modèle figurant à l'annexe 1 des présentes Lignes directrices (accès autorisé

uniquement aux agents de la DIO), dans la mesure du possible. Les informations contiennent au minimum une brève description des faits relatifs à la violation des données à caractère personnel et de ses effets probables.

6.6 Le directeur ou la directrice de la DIO notifie la personne déléguée à la protection des données, comme le prévoit le Règlement. Après réception du rapport mentionné au paragraphe précédent, le directeur ou la directrice de la DIO décide, au cas par cas et au vu du contenu et de la nature de la violation ainsi que des impératifs de confidentialité de la DIO, quelles données seront incluses dans la notification. Dans cette notification, le directeur ou la directrice de la DIO peut également demander que la personne déléguée à la protection des données reporte temporairement la notification qui doit être faite à la personne concernée, en vertu de l'article 6, paragraphe 5, du Règlement, si cela se justifie (par exemple, si la confidentialité d'un processus d'investigation doit être préservée ou s'il existe d'autres raisons dûment justifiées). Le cas échéant, la DIO fournit sur demande toute information nécessaire pour permettre à la personne déléguée à la protection des données de se forger une opinion sur la question.

6.7 Une fois l'obligation de notification des violations de données remplie, dans la mesure du possible, la fonction dans le cadre de laquelle la violation de données s'est produite doit fournir au directeur ou à la directrice de la DIO une analyse des causes de la violation de données et suggérer des mesures d'atténuation adéquates. Le directeur ou la directrice de la DIO peut examiner les méthodes de travail et recommander des mesures à mettre en œuvre pour prévenir d'autres violations de données. La personne déléguée à la protection des données est informée des mesures prises à cet effet.

6.8 La DIO tient un registre de violation des données, tel qu'il figure à l'annexe 2 ci-après (accès autorisé uniquement aux agents de la DIO).

Article 7

Transparence du traitement des données

7.1 La DIO communique à la personne dont les données font l'objet d'un traitement (la « personne concernée ») les informations visées à l'article 7 du Règlement sur la protection des données, si elle ne dispose pas déjà de ces informations, excepté si les données à caractère personnel ne sont pas collectées auprès de la personne concernée elle-même ou si cela s'avère impossible, ou encore si cela implique des efforts disproportionnés ou risque de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement. Compte tenu de la nature des activités et du mandat de la DIO dans le cadre d'évaluations, de missions d'assurance (audit), de missions de consultance et de processus d'investigation, la DIO peut être amenée à recourir aux restrictions prévues à l'article 10 du Règlement, notamment pour ce qui concerne le droit à l'information de la personne concernée.

Article 8

Droits de la personne concernée

8.1 Toute personne dont les données à caractère personnel sont traitées par la DIO bénéficie des droits inscrits aux articles 7 et 8 du Règlement du Conseil de l'Europe sur la protection des données. Toutefois, compte tenu de la nature de ses activités dans le cadre d'évaluations, de missions d'assurance (audit), de missions de consultance et de processus d'investigation, la DIO peut avoir recours aux restrictions prévues à l'article 10 du Règlement sur la protection des données.

Article 9

Obligations complémentaires

9.1 La réalisation du traitement des données par un tiers/sous-traitant pour le compte de la DIO est subordonnée à l'assurance de garanties adéquates en matière de respect du niveau de protection prévu dans le cadre juridique de l'Organisation. Dans ce cas, l'accord énonce les principaux aspects relatifs au traitement, notamment sa nature et sa finalité, sa durée, le type de données à caractère personnel traitées, les catégories de personnes concernées et les obligations ainsi que les droits de l'Organisation et du sous-traitant.

9.2 Tout sous-traitant agissant pour le compte de la DIO se voit remettre les présentes Lignes directrices et est tenu de respecter leurs dispositions pertinentes, qui s'appliquent mutatis mutandis. En tant que responsable du traitement des données, la DIO conserve le droit exclusif d'imposer des restrictions aux droits des personnes concernées dans le cadre de ses activités ; en d'autres termes, le sous-traitant est informé que des restrictions ne peuvent être imposées qu'après approbation de la DIO et conformément au Règlement et aux présentes Lignes directrices du Conseil de l'Europe.

9.3 Compte tenu de la spécificité des besoins et du mandat du DIO, la structure, le contenu et les méthodes d'accès aux dossiers conservés par les responsables du traitement en vertu de l'article 9, paragraphe 8, du Règlement sont détaillés et convenus avec la personne déléguée à la protection des données.

Article 10

Restrictions

10.1 Comme le prévoient les présentes Lignes directrices, la DIO peut recourir à l'application des restrictions aux articles 7 et 8 du Règlement prévues à l'article 10.

10.2 Dans des cas spécifiques, le recours à des restrictions peut être nécessaire et proportionné pour que la DIO remplisse son rôle, qui comprend la protection d'intérêts financiers importants de l'Organisation, ainsi qu'en matière de responsabilité, de transparence, de prévention des violations du cadre juridique interne et/ou des lois applicables, ou d'investigations concernant ces violations, et de conduite de procédures disciplinaires.

10.3 Pour garantir le respect des droits et des libertés fondamentales des personnes concernées, l'adoption de toute mesure de ce type requiert une explication écrite des motifs justifiant la nécessité de la mesure. Cependant, étant donné que, conformément au cadre juridique de l'Organisation, les processus d'investigation sont confidentiels et que la personne faisant l'objet d'une investigation doit être informée dans les plus brefs délais, tout en veillant à ce que cela ne compromette pas le recueil de preuves, la notification de la personne concernée, pouvant être considérée comme la personne faisant l'objet de l'investigation, peut être reportée, en principe, jusqu'à ce qu'elle soit jugée opportune.

10.4 Les restrictions ne sauraient équivaloir à un déni pur et simple des droits prévus par le Règlement et leur nécessité doit être réévaluée régulièrement. De plus, comme le prévoient les présentes Lignes directrices et conformément au Règlement, dans la mesure du possible, toute restriction doit être :

- adoptée à titre temporaire ;
- décidée au cas par cas ;
- applicable à un ou plusieurs droits, selon les circonstances de l'espèce ;
- imposée uniquement après que le responsable du traitement a effectué un test de nécessité et de proportionnalité ;
- documentée dans un dossier écrit interne et confidentiel ;
- appliquée uniquement lorsque des garanties ont été mises en place pour prévenir l'utilisation abusive, l'accès, la transmission ou le transfert illicites de données à caractère personnel.

10.5 Les restrictions au droit d'être informé du traitement des données peuvent comprendre, dans le cadre d'un processus d'investigation, un délai dans la communication d'informations à une personne concernée spécifique ou la réalisation de l'obligation d'informer uniquement par des moyens tels que des liens appropriés dans la signature électronique de courriel et la mention du traitement des données dans les lettres de mission.

10.6 Les restrictions du droit d'accès aux données à caractère personnel dans le cadre d'un processus d'investigation peuvent inclure, par exemple, un délai avant de confirmer le traitement des données à la demande de la personne concernée.

10.7 Sans préjudice des droits reconnus aux personnes concernées à l'article 18 du Règlement, les personnes concernées qui se voient notifier une ou plusieurs restrictions de leurs droits dans le cadre des activités de la DIO peuvent introduire une demande motivée de réexamen. La demande est adressée au directeur ou à la directrice de la DIO dans les trente jours ouvrables suivant la notification. Toutes les demandes doivent inclure ou faire précisément référence à la notification de la restriction ainsi que tout autre élément (documents, déclarations, etc.) susceptible d'aider la DIO à réexaminer et à réévaluer la restriction.

Article 11

Non-respect des obligations par des agents et autres membres du Secrétariat

11.1 Outre les obligations imposées par l'article 11 du Règlement, les membres du Secrétariat donnent à la DIO un accès direct et rapide aux données à caractère personnel concernant des membres du Secrétariat et d'autres personnes participant aux activités du Conseil de l'Europe à quelque titre que ce soit, lorsque cela est nécessaire, proportionné et demandé.

11.2 La DIO a accès en temps voulu et sans restriction à d'autres documents pertinents qu'elle juge nécessaires à l'accomplissement de ses tâches, conformément à l'article 12 de la Charte de la DIO. Le refus de répondre à une demande de la DIO doit être dûment motivé par la partie concernée. Les agents de la DIO invitent la partie concernée à fournir des arguments détaillés expliquant pourquoi le traitement des informations demandées par la DIO ne serait pas conforme aux principes de légalité, de nécessité, de proportionnalité et d'adéquation. Si nécessaire, la personne déléguée à la protection des données est invitée à donner son avis en cas de refus.

Article 12

Transfert de données à caractère personnel à des tiers

12.1 Le transfert de données à caractère personnel en dehors de l'Organisation vers un destinataire relevant de la compétence d'un État, une autre organisation internationale et les institutions, organes, bureaux et agences de l'UE est soumis aux exigences et aux garanties énoncées à l'article 12, paragraphe 1, du Règlement sur la protection des données. La notion de destinataire relevant de la compétence d'un État inclut notamment les consultants et les donateurs privés qui participent aux activités du Conseil de l'Europe.

12.2 La décision concernant l'application de garanties particulières en vue d'assurer le niveau de protection adéquat au sens de l'article 12, paragraphe 1, du Règlement sur la protection des données est prise après consultation de la personne déléguée à la protection des données.

12.3 Des consultations spécifiques avec la personne déléguée à la protection des données sont menées pour évaluer le niveau de protection requis par le Règlement sur la protection des données dans le cadre d'évaluations et d'audits conjoints.

12.4 Le renvoi aux autorités nationales dans le cadre d'un examen préliminaire ou d'une investigation peut être effectué en dehors des garanties, d'après l'article 12, paragraphe 3, point 4, du Règlement sur la protection des données et dans le respect du cadre juridique de l'Organisation. Dans tous les cas, la DIO veille avec le plus grand soin à assurer un niveau adéquat de protection des droits de la ou des personnes concernées.

12.5 La DIO peut communiquer à la personne déléguée à la protection des données certaines informations relatives au transfert de données qui relèvent de l'article 12, paragraphe 4, des présentes Lignes directrices. La décision de communiquer ou non les informations et la portée des informations communiquées sont établies au cas par cas par le directeur ou la directrice de la DIO, compte tenu de la confidentialité de certaines activités de la DIO.

12.6 La DIO traite au cas par cas toute demande concernant l'accès aux données à caractère personnel. Si la demande émane d'un auditeur externe, la personne déléguée à la protection des données est consultée tant pour ce qui concerne la réponse que toute modalité de communication des informations demandées ; la consultation peut ne pas être nécessaire si la personne déléguée à la protection des données et la DIO conviennent de la manière de procéder pour les demandes d'informations récurrentes/standards formulées par les auditeurs externes du CdE.

12.7 La procédure de coordination peut être omise si tous les acteurs concernés conviennent d'une procédure de réponse standard pour les demandes fréquentes et standardisées.

12.8 La DIO tient un registre des demandes d'accès aux données et des suites apportées, tel qu'il figure à l'annexe 3 des présentes Lignes directrices (accès autorisé uniquement aux agents de la DIO).

Article 13

Personne déléguée à la protection des données

13.1 Outre les cas dans lesquels un accord avec la personne déléguée à la protection des données est déjà prévu, tel que mentionné dans les présentes Lignes directrices, la DIO coordonne et clarifie avec la personne déléguée à la protection des données, chaque fois que nécessaire, les questions liées à la protection des droits des personnes concernées et au traitement des données à caractère personnel.

13.2 Tous les échanges sont consignés par écrit dans le Registre prévu à cet effet pour référence ultérieure, tel qu'il figure à l'annexe 4 des présentes Lignes directrices (accès autorisé uniquement aux agents de la DIO). Les échanges contenant des données à caractère personnel sont dûment expurgés avant d'être enregistrés au cas où ils contiendraient des données dont la communication à des personnes ne participant pas à des

activités spécifiques n'est pas autorisée (dans le cadre d'examens préliminaires et d'investigations, par exemple).

13.3 Dans le cadre de ses activités, la DIO peut être amenée à recourir à des mesures provisoires en matière de protection des données, c'est-à-dire à des solutions temporaires en l'absence d'accord ou d'avis spécifique émanant de la personne déléguée à la protection des données. Dans tous les cas, les solutions temporaires tiennent compte des droits reconnus aux personnes concernées par le Règlement et des principes contenus dans les orientations reçues précédemment. Elles peuvent être adoptées lorsqu'il n'est pas possible d'établir un contact préalable avec la personne déléguée à la protection des données ou lorsqu'un avis est attendu, mais n'a pas encore été rendu ; elles ne dispensent pas la DIO de l'obligation visée à l'article 13, paragraphe 1, des présentes Lignes directrices.

13.4 Les solutions temporaires appliquées au moment de l'entrée en vigueur des Lignes directrices figurent à l'annexe 5 des présentes (accès autorisé uniquement aux agents de la DIO). D'autres solutions temporaires et toute mise à jour de celles mentionnées aux annexes sont consignées et rendues accessibles conformément aux modalités décrites à l'article 13, paragraphe 2, des présentes Lignes directrices.

Article 14

Entrée en vigueur

14.1 Les présentes Lignes directrices concernant l'application du Règlement du Conseil de l'Europe sur la protection des données dans le cadre des activités de la Direction de l'Audit interne, de l'Évaluation et de l'Investigation prennent effet le 1er janvier 2023.

Article 15

Mesures transitoires

15.1 Le directeur ou la directrice de l'Audit interne, de l'Évaluation et de l'Investigation veille à ce que le traitement de données à caractère personnel déjà en cours à la date d'effet des présentes Lignes directrices soit mis en conformité avec celles-ci dans un délai raisonnable.

Annexe 1 – Note au dossier de signalement de violations de données

[Lien DMS vers le document]

DIRECTORATE OF INTERNAL OVERSIGHT

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Note
For the attention of Mr/ Mrs…….—Director of the Directorate of Internal Oversight (DIO)
Subject: Report of personal data breach

Name and surname	Description of the breach*
Job title	
Date of the discovery	
Date of reporting of the incident (DIO)	
Date of reporting to the DPO	
Data subjects involved (number/categories)	
Number of data files/records involved	
Possible reasons for the breach	
Actions taken	
Further actions (proposed/recommended/needed)	
Estimated impact of the breach	
Comments	

Documents (if applicable)

Annexe 2 – Modèle de Registre des violations de données

Lien DMS vers le document

Numbe	Year	Function	Date of discovery	Director informed?	Date of reporting	DMS link to the note	DPO contacted?	Date of DPO contact	DMS link to communication with the DPO	Actions taken	Actions to be taken	Notes
1	2023	AUD	01/01/2023	Yes	01/01/2023		Yes	01/01/2023				
		EVAL		No			No					
		INV										
		Multiple										

Annexe 3 – Modèle de Registre des demandes d'accès aux données

Lien DMS vers le document

Ref. Nb	Year	Function concerned	Date of request	Date received	Person/entity who submitted the request	DMS link to the request	Director informed	DPO contacted	Date of DPO contact	DMS links to the exchanges with the DPO	DPO's opinion (main point/s)	Actions taken	Date of reply/closure	Comments
1	2023	AUD	01/01/2023				Yes	Yes	01/01/2023					
		EVAL					No	No						
		INV												
		Multiple												

Annexe 4 – Modèle de Registre des échanges avec la personne déléguée à la protection des données

Lien DMS vers le document

Summary of the question from DIO	Date of submission of the question	Summary of the answer from DPO	Date of receipt of the answer	DMS link to the exchange documents
Text	01/01/2023	Text	01/01/2023	Link
Text	01/01/2023	Text	01/01/2023	Link
Text	01/01/2023	Text	01/01/2023	Link
Text	01/01/2023	Text	01/01/2023	Link

Annexe 5 – Liste des solutions temporaires employées actuellement par la DIO (1er janvier 2023)

Lien DMS vers le document

Description	Solution
INV : signature utilisée dans les premiers contacts par courriel	Veuillez noter que les informations concernant la protection des personnes à l'égard du traitement automatisé des données à caractère personnel par le Conseil de l'Europe peuvent être consultées à l'adresse suivante : https://www.coe.int/fr/web/data-protection/data-protection-commissioner Le présent message et toute pièce qui y est jointe sont confidentiels et destinés exclusivement à son ou ses destinataires. S'il vous est parvenu par erreur, veuillez en informer immédiatement l'expéditeur et détruire ce message. Toute modification ou diffusion du présent message est interdite.
EVAL : texte joint à l'invitation à répondre à une enquête dans le cadre d'une évaluation	Pour toute question relative à la manière dont vos données sont collectées et utilisées, veuillez contacter le Conseil de l'Europe par courriel : soit à [nom de l'agent EVAL] à l'adresse suivante : [courriel de l'agent EVAL] ; soit à la personne déléguée à la protection des données du Conseil de l'Europe à l'adresse suivante : dpo@coe.int.