	DOCUMENTATION ISMS	
LOTERIE ROMANDE	**Type de document :** Politique	**Propriétaire :** Directrice du Département des Affaires Juridiques
	Classification : Interne	

ISMS_24_POLITIQUE PROTECTION DES DONNEES LPD_V3.0.docx

Rôles & Responsabilités dans le cadre de ce document

Responsable	Directrice du Département des Affaires Juridiques
Auditeurs	Audit interne ou externe
Participants	Départements Affaires juridiques, Ressources Humaines, Département DOSI et Contrôle de Gestion
Informés	Ensemble des collaborateurs LoRo
Demandeur	Direction Générale
Ecrivain, éditeur	Affaires Juridiques

Table des matières

1 Sommaire à l'intention du lecteur

1.1 Description et objectifs du document

La présente politique définit les mesures prises et le système mis en place par la Loterie Romande pour assurer la gestion de la protection des données.

Elle vise ainsi à assurer la conformité de l'organisation et de l'exécution des traitements de données avec les exigences légales, à identifier, analyser et prévenir les risques de non-conformité et/ou à remédier aux situations de non-conformité.

Cette politique a été développée sur la base des dispositions contenues dans la loi sur la protection des données (LPD) et son ordonnance d'application (OLPD), ainsi que de l'article 328b du Code des Obligations (CO).

Elle tient compte en plus de certaines dispositions prévues par les *Directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir* du 19 mars 2014, ainsi qu'à l'annexe y relative du 15 avril 2014.

1.2 Périmètre d'application

Font partie du périmètre d'application toutes les informations qui se rapportent à une personne identifiée ou identifiable.

Recommandation pratique – On peut citer les exemples suivants :
- Les données personnelles relatives aux collaborateurs déployant ou ayant déployé une activité pour la Loterie Romande
- Les données personnelles relatives aux candidats qui postulent à un poste de travail à la Loterie Romande
- Les données personnelles relatives aux personnes participant aux jeux (joueurs) proposés par la Loterie Romande
- Les données personnelles relatives aux joueurs gagnants aux jeux proposés par la Loterie Romande
- Les données personnelles relatives aux dépositaires à qui la Loterie Romande confie la commercialisation de ses jeux.

1.3 Association avec les normes ISO 27001 et WLA

Cette politique supporte les contrôles ISO 27001 et WLA-SCS suivants :

8.1.4	Modifications imprévues
A.13.2.2	Accords en matière de transfert d'information
A.14.3.1	Protection des données de test
A.15.1.2	La sécurité dans les accords conclus avec les fournisseurs
A.18.1.1	Identification de la législation et des exigences contractuelles applicables
A.18.1.4	Protection de la vie privée et protection des données à caractère personnel
G.5.2.1	Méthodologie et données de test

2 Cadre général

2.1 But de la politique

La présente politique concrétise les mesures prises et le système mis en place par la Loterie Romande pour assurer la **gestion** de la protection des données (ci-après la politique).

Commentaire juridique
La gestion de la protection des données vise ainsi à assurer la **conformité** de l'organisation et de l'exécution des traitements de données avec les exigences légales, à identifier, analyser et prévenir les risques de **non-conformité** et/ou à remédier aux situations de non-conformité.

Recommandation pratique – gérer la conformité
En cas de projet impliquant un traitement de données (que ce soit un projet purement interne ou un projet impliquant la collaboration d'un tiers), il est recommandé de s'adresser au département juridique, à la direction des technologies de l'information et, le cas échéant, au Conseiller à la Protection des Données pour évaluer la conformité du traitement de données projeté, prendre les précautions nécessaires et, le cas échéant, élaborer ou réviser les contrats.
Exemples : Un projet visant à **analyser des données** à des fins marketing ou à des fins de prévention du jeu excessif et/ou la **délégation de traitements de données** à un tiers (outsourcing) et/ou le **transfert de données à l'étranger** répondent à des exigences spécifiques qu'il y a lieu d'évaluer et de prendre en compte.

Recommandation pratique – gérer la non-conformité
En cas d'événement, de situation ou d'incident indiquant la possibilité d'une violation des exigences légales et/ou des directives internes en matière de protection des données, les collaborateurs signalent immédiatement l'incident via l'outil 888 pour permettre aux Directeurs du département concerné, du Contrôle de Gestion, des technologies de l'information, du département juridique et le cas échéant au Conseiller à la Protection des Données, de prendre les dispositions nécessaires pour identifier, analyser et remédier aux situations de non-conformité (voir ci-dessous ch. 6).

2.2 Cadre légal et exigences applicables

La politique vise à assurer le respect des exigences **légales** posées essentiellement par la loi fédérale sur la protection des données (LPD[1]) et par son ordonnance d'application (OLPD[2]).

Commentaire juridique
Les exigences légales résultant de la LPD et de l'OLPD ont pour but de protéger la **personnalité** et les **droits fondamentaux** des personnes qui font l'objet d'un traitement de données. La base de cette protection résulte de la **constitution fédérale**[3] et du **code civil**[4]. Selon les domaines, les exigences peuvent cependant découler d'autres lois spéciales : par exemple, dans les rapports de travail, il y a lieu de tenir compte du **code des obligations**[5], de la **loi sur l'égalité**[6] et de la **loi sur le travail**[7].

[1] *RS 235.1.*
[2] *RS 235.11.*
[3] *RS 101 : art. 13 al. 2 Cst. (droit à l'autodétermination informationnelle).*
[4] *RS 210 : art. 28 CC (protection de la personnalité)*
[5] *RS 220 : art. 328b CO (traitement de données concernant les travailleurs).*
[6] *RS 151.1 : notamment art. 8 al. 2 LEg (durée de conservation des données pour répondre à d'éventuelles prétentions).*
[7] *RS 822.11 : art. 6 al. 1 LTr (protection de l'intégrité personnelle des travailleurs) ; RS 822.113 : art. 2 al. 1 OLT 3 (protection de la santé physique et psychique des travailleurs) et art. 26 OLT 3 (surveillance des travailleurs).*

Recommandation pratique – identifier le cadre légal et les exigences applicables
En cas de doute sur les exigences légales applicables à un traitement de données personnelles projeté, il est recommandé de s'adresser au département juridique, à la direction des technologies de l'information et, le cas échéant, au Conseiller à la Protection des Données pour identifier le cadre légal et les exigences spécifiquement applicables.
Exemples : Pour l'installation d'une **vidéosurveillance** ou d'autres systèmes de **surveillance sur le lieu de travail**, il y a lieu de prendre en compte les exigences de la législation sur la protection de la santé au travail ; pour l'**archivage légal**, il y a lieu de prendre en compte la législation en matière de tenue et conservation des livres et d'identifier également les normes de responsabilités applicables afin de définir les types de fichiers et les durées de conservation pertinentes (voir également la directive ISMS 142 de conservation des documents et de l'information)

3 Définitions

Les définitions des principaux termes utilisés dans la politique sont les suivantes[8] :

3.1 Données personnelles (données)

Toutes les informations qui se rapportent à une personne identifiée ou identifiable.

3.2 Personne concernée

Personne physique ou morale au sujet de laquelle des données sont traitées.

3.3 Données sensibles

Données personnelles sur :

- opinions ou activités religieuses, philosophiques, politiques ou syndicales
- santé, sphère intime ou appartenance à une race
- mesures d'aide sociale
- poursuites ou sanctions pénales et administratives

Commentaire juridique
Les **données sensibles** font l'objet de **dispositions spécifiques** et d'une protection spéciale dans la loi fédérale sur la protection des données (LPD), notamment en matière de consentement (art. 4 al. 5), de déclaration de fichiers (art. 11a al. 3 let. a), d'information lors de la collecte de données (art. 14), de communication à des tiers (art 12 al. 2 let. c).

Recommandation pratique – identifier les données sensibles
En cas de doute sur le point de savoir si l'on est en présence d'une **donnée sensible** et pour identifier le **niveau de protection à respecter** et les précautions à observer en matière de sécurité (voir ci-dessous ch. 5.7), il est recommandé de s'adresser au directeur du département concerné, au département juridique, à la direction des technologies de l'information et, le cas échéant, au Conseiller à la Protection des Données.
Exemples :
Les données relatives aux poursuites ou sanctions **administratives et pénales** sont notamment : celles rendues en matière **fiscale**, celles concernant le **casier judiciaire** ou le **permis de conduire**. En revanche, les décisions en matière de **dettes et faillite** ou en matière **civile** ne sont techniquement pas des données sensibles, notamment : **saisie de salaire**, **avis au débiteur**, **mesures de protection de l'adulte**; il y a toutefois lieu de les traiter comme des données sensibles et avec un haut degré de confidentialité. Il en va de même des **données relatives au revenu et à la fortune** qui, d'un point de vue technique, ne constituent pas non plus des données sensibles ; cependant, les **données personnelles relatives aux gagnants** doivent être traitées avec un haut degré de confidentialité, conformément au principe de **proportionnalité** (voir ci-dessous ch. 5.3) : plus les gains sont élevés, plus le degré de confidentialité à respecter doit être élevé.

[8] *Ces définitions correspondent à celles prévues par l'art. 3 de la loi fédérale sur la protection des données (LPD).*

3.4 Profil de la personnalité

Assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique

3.5 Traitement

Toute opération relative à des données personnelles - quels que soient les moyens et procédés utilisés - notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données

3.6 Communication

Fait de rendre des données personnelles accessibles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant

3.7 Fichier

Tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée

3.8 Maître du fichier

La personne qui décide du but et du contenu du fichier

Commentaire juridique
Le **maître du fichier** (ou « propriétaire » des données) est la personne qui a le **contrôle de fait** sur les données, et qui est considérée comme le **responsable primaire** de leur traitement ; le maître du fichier peut être une personne morale ou une personne physique. C'est le maître du fichier qui a le pouvoir de décider de la **création d'un fichier** de données, d'en déterminer le **but**, de définir les **catégories données** traitées et les **moyens techniques** à utiliser ; ce pouvoir peut être **exclusif ou partagé**. Le maître du fichier assume des **obligations spécifiques**, notamment en matière de déclaration de fichier (art. 11a al. 3 LPD), de communication transfrontière de donnée (art. 6 al. 2 let. a et g LPD), de devoir d'information (art. 14 LPD), de droit d'accès (art. 8 LPD), de sécurité (art. 7 LPD).

Recommandation pratique – identifier le maître du fichier
Le maître du fichier est la Société de la Loterie de la Suisse Romande. En pratique, la responsabilité de maître du fichier au sein de l'entreprise est **partagée** entre le **directeur de chaque département**, qui a le droit de décider de la création de nouveau fichier, et le **directeur du département juridique et la direction des technologies de l'information**, qui sont compétents pour toutes les autres obligations qui incombent techniquement au maître du fichier.
Exemple :
Pour chaque département, la décision de créer un nouveau fichier de données ne peut être prise que par le directeur du département, qui est la personne habilitée, c'est-à-dire autorisée à le faire par le maître du fichier.

4 Rôles et responsabilités

4.1 Maître du fichier

- Le maître du fichier est l'organisme désigné au sein de la Loterie Romande comme le responsable de tous les traitements de données effectués.
- Le maître du fichier a pour mission de déterminer l'objectif, le contenu et l'accès aux données personnelles des collaborateurs traitées par les Ressources humaines et des données des joueurs traitées par la Loterie Romande. A cet effet, le maître du fichier est notamment habilité à :
    - accorder ou non l'accès à des données personnelles via l'application Gespriv
    - enregistrer les déclarations signées par les bénéficiaires d'un profil d'accès lors de l'octroi d'une autorisation
    - prendre toutes les mesures nécessaires et utiles afin de garantir la confidentialité et l'exactitude des données concernées
    - proposer la modification des profils d'accès

4.2 Collaborateurs (participants à un traitement)

- Tout collaborateur au bénéfice d'un profil d'accès ou d'une autorisation accordée par le maître du fichier est tenu d'assurer la protection des données auxquelles il accède.
- Il est tenu d'utiliser les données strictement dans le but qui leur est dévolu.
- Il n'est autorisé à communiquer lesdites données à des tiers que moyennant respect des règles définies dans le guide pratique (autorisation expresse du Département des ressources humaines ou du Département Juridique et signature d'une clause de confidentialité).
- Toute violation des règles de protection des données impliquera le blocage du profil d'accès. Tout contrevenant se verra en outre appliquer les sanctions internes adéquates, pouvant aller de l'avertissement au licenciement. D'éventuelles sanctions pénales demeurent réservées.

4.3 Personnes concernées

- Les personnes concernées par des traitements de données à la loterie Romande sont notamment les suivantes :
    - collaborateurs
    - candidats
    - joueurs
    - gagnants
    - dépositaires
- Selon les dispositions légales et/ou contractuelles applicables, les personnes concernées sont responsables de fournir l'intégralité des données personnelles requises par la Loterie Romande et d'en garantir l'exactitude; elles sont tenues d'annoncer sans délai tout changement relatif à leur situation personnelle.
- Les personnes concernées sont dûment informées que toute fausse déclaration ou toute dissimulation de données utiles engage leur responsabilité personnelle.

Recommandation pratique – « Guide pratique »
Afin de compléter les indications ressortant de la présente politique, la Loterie Romande a prévu d'y annexer un « Guide pratique » contenant des directives et recommandations complémentaires destinées aux collaborateurs qui participent à des traitement de données personnelles, afin de préciser et concrétiser les mesures et précautions à observer en rapport avec les traitements de données qui leur sont confiés.

4.4 Conseiller à la Protection des Données

- Les entreprises privées qui traitent régulièrement des données sensibles ou des profils de la personnalité sont tenues de déclarer leurs fichiers au Préposé fédéral à la protection des données et à la transparence[9]. Pour être déliées de ce devoir, elles peuvent désigner un Conseiller à la Protection des Données et l'annoncer au Préposé fédéral à la protection des données et à la transparence, ce que la Loterie Romande a fait en désignant en cette qualité, l'un de ses conseillers juridiques externes, Me Charles Joye, avocat à Lausanne.
- Le Conseiller à la Protection des Données doit disposer des connaissances et des qualifications professionnelles nécessaires, que ce soit dans le domaine de la législation sur la protection des données ou dans celui des normes techniques (par ex. ISO 27001, ISO 17799, etc.). Il ne doit pas exercer d'activités incompatibles avec ses tâches de Conseiller à la Protection des Données (principe d'indépendance).
- Le Conseiller à la Protection des Données peut être un membre du personnel de l'entreprise ou un tiers ; s'il est un collaborateur de l'entreprise, il ne pas être intégré dans la hiérarchie directe (notamment être le responsable des systèmes d'information, de la clientèle ou des ressources humaines) ; en revanche, il peut être rattaché au service juridique ou au chargé de sécurité informatique. La fonction de Conseiller à la Protection des Données peut aussi être confiée à une personne ou à une équipe composée d'un spécialiste de la protection des données et d'un spécialiste en matière de sécurité informatique.
- Le Conseiller à la Protection des Données assume un rôle d'assistance et de contrôle. Il contribue à l'inventaire des fichiers, à l'analyse des risques et propose des mesures si des prescriptions ont été violées[10]. Il a également pour mission de conseiller et former le personnel, de donner son avis sur les projets internes impliquant des traitements de données et effectue des audits internes périodiques sur le niveau de protection et les difficultés de mise en œuvre. Ainsi, le Conseiller à la Protection des Données exerce notamment les tâches suivantes :
  - contrôler les traitements des données personnelles effectués
  - proposer les corrections nécessaires en cas de violation des prescriptions sur la protection des données
  - dresser l'inventaire des fichiers soumis à déclaration selon l'art. 11a al. 3 LPD
  - conseiller et former le personnel en édictant des directives ou des instructions
  - émettre des recommandations à l'intention du maître du fichier
- Le Conseiller à la Protection des Données doit pouvoir connaître les fichiers et traitements de données (uniquement ceux qui entrent dans le champ d'application de la loi), ainsi que l'organisation et les normes et systèmes de l'entreprise en ce domaine. Il doit pouvoir obtenir les documents et renseignements nécessaires de la part des personnes responsables du traitement des données.

4.5 La sécurité

- L'entité » sécurité » rattachée au département du Contrôle de Gestion, est responsable de la mise en place et du maintien du Système de Management de la Sécurité de l'Information (SMSI). A ce titre elle participe à la mise en place des mesures de protection des données via l'élaboration des documents et les mesures de sensibilisation qui accompagnent sa diffusion.

4.6 L'audit interne ISO

- L'entité « Audit interne ISO », rattachée au département du Contrôle de Gestion, vérifie la conformité des processus de travail en place avec les mesures prévues dans cette politique.

[9] *Art. 11a al. 3 LPD.*

[10] *Le conseiller n'a pas le droit de communiquer au Préposé fédéral à la protection des données et à la transparence l'existence de violation des règles de protection des données ou le fait que ses recommandations ne seraient pas suivies.*

4.7 Direction des technologies de l'information

- La direction des technologies de l'information est responsable de la mise en œuvre, de la gestion et de la maintenance des différents systèmes d'informations, ainsi que de l'analyse et de la résolution de leurs dysfonctionnements, conformément à la présente politique et à la politique générale de sécurité de la Loterie Romande.

5 Principes généraux de la protection des données

Tout traitement de données personnelles doit respecter les principes généraux de la protection des données[11], qui sont les suivants :

5.1 Licéité

Le traitement de données doit être licite, c'est-à-dire conforme au droit[12] : le **principe** du traitement doit être licite, de même que ses **modalités** (c'est-à-dire dans la manière avec laquelle il est réalisé) et son **étendue** (notamment la quantité de données traitées et la durée de leur conservation).

a) Motifs justificatifs

Pour être licite, le traitement de données personnelles doit se fonder sur un motif justificatif, c'est-à-dire sur un motif qui légitime ce traitement. Ce motif peut s'appuyer sur le **consentement** de la personne dont les données sont traitées, sur un **intérêt prépondérant** (privé ou public) ou sur la loi[13].

i) Consentement

- Le consentement n'est valable que s'il est **libre et informé** : le consentement doit être donné en l'absence de toute contrainte pour la personne et sur la base d'une information claire qui lui permette de mesurer le risque d'atteinte à sa personnalité engendré par le traitement de ses données.
- Lorsque le traitement porte sur des **données sensibles**[14] ou sur des **profils de personnalité**[15] le consentement doit être **explicite**[16], qui paraît possible par actes concluants, notamment en cochant une case dédiée dans la procédure d'enregistrement permettant l'utilisation d'une plateforme Internet.

ii) intérêt public

- L'intérêt public prépondérant est un intérêt destiné à procurer un avantage à la collectivité ou à une pluralité de personnes, par exemple en matière de sécurité ou de santé publique ; il est en général concrétisé par une norme légale et vient souvent appuyer l'existence d'un intérêt privé au traitement.

iii) intérêt privé

- L'intérêt privé prépondérant doit être digne de protection ; il peut être celui de la personne concernée, d'un tiers ou de l'auteur du traitement ; un tel intérêt justifie existe notamment pour le traitement de données en relation directe avec la **conclusion** ou l'**exécution d'un contrat**[17].

[11] *Art. 4, 5 et 7 LPD.*
[12] *Art. 4 al. 1 LPD.*
[13] *Art. 13 al. 1 LPD.*
[14] *Art. 3 let. c LPD.*
[15] *Art. 3 let. d LPD.*
[16] *Art. 4 al. 5 LPD.*
[17] *Art. 13 al. 2 let. a LPD.*

Commentaire juridique
Pour ce qui est du respect de l'exigence de licéité, les traitements de données qui entrent dans le champ d'application de la présente politique sont en principe justifiés par les nécessités liées à la conclusion et à l'exécution des contrats que la Loterie Romande passe avec ses **joueurs**, **collaborateurs**, **dépositaires** et **fournisseurs** ; les exigences découlant des autres principes doivent également être respectées. Parmi les autres **intérêts privés prépondérants** qui peuvent être pris en considération, on peut citer : le traitement concernant un rapport de **concurrence économique** avec une autre personne (art. 13 al. 2 let. b); celui effectué pour **évaluer le crédit** d'une autre personne (art. 13 al. 2 let. c); celui effectué à des fins de **recherche, planification ou statistique** (art. 13 al. 2 let. e).

Recommandation pratique – identifier le motif justificatif et sa portée
Pour chaque traitement de données personnelles, il y a lieu d'identifier le motif justificatif qui légitime ce traitement. Si le motif est le consentement de la personne intéressée, il y a lieu de s'assurer que ce consentement a été obtenu sur la base d'une information suffisante. Si le motif justificatif résulte d'un intérêt prépondérant privé (notamment d'un contrat) ou public, il y a lieu de s'assurer que cet intérêt peut être rendu vraisemblable, et que, dans le cadre d'une pesée des intérêts, il peut effectivement légitimer l'éventuelle atteinte à la personnalité pouvant résulter du traitement de données opéré sur la base de ce motif. En cas de doute sur l'existence et la validité d'un motif justifiant un traitement de données personnelles, surtout si le traitement porte sur des données sensibles ou peut être assimilé à un profil de personnalité, il est recommandé de s'adresser au département juridique, au département du Contrôle de Gestion, à la direction des technologies de l'information et, le cas échéant, au Conseiller à la Protection des Données.
Exemples : Un **projet marketing** impliquant le traitement de données personnelles de joueurs visant à dégager leur **profil de joueurs** exige de vérifier si ce traitement repose sur un motif justificatif suffisant, en particulier s'il est légitimé par un consentement explicite des intéressés obtenu sur la base d'une information suffisamment précise.

b) Traitement de données par un tiers

Le traitement de données personnelles peut être délégué à un tiers (outsourcing) si une convention le prévoit, étant précisé que seuls les traitements que le mandant serait en droit de réaliser sont effectués, et qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdit ; le mandant s'assure que le tiers garantit la sécurité des données[18].

Commentaire juridique
Lorsque les conditions posées par la loi indiquées ci-dessus sont respectées, l'outsourcing ne nécessite en principe ni information ni consentement ; un consentement n'est nécessaire que si, et dans la mesure où, ces conditions ne seraient pas respectées. La convention traite aussi des questions relatives aux **technologies et systèmes** utilisés, **accès**, **développement** et **maintenance** des bases de données, **localisation** du matériel, lieu d'où les services sont fournis, **instructions**, **contrôles** et **audits**, **conservation** et **archivage**.

Recommandation pratique – prévoir une convention
La délégation de certains traitements de données exige une **convention** écrite, qui précise notamment le type et l'étendue des **traitements délégués**, les mesures prises aux fins de garantir la **confidentialité** et la **sécurité**. Le maître du fichier doit choisir un délégataire qui apporte des **garanties suffisantes** quant aux **mesures de sécurité technique et organisationnelles** nécessaires à l'encadrement des traitements de données à effectuer et doivent veiller au respect de ces mesures. Afin de régler les modalités contractuelles nécessaires à mettre en place une délégation de traitement de données, il est recommandé de s'adresser au département juridique, au département du Contrôle de

[18] *Art. 10a LPD.*

Gestion, à la direction des technologies de l'information et, le cas échéant, au Conseiller à la Protection des Données.

5.2 Transparence

- Le traitement de données doit être accompli de manière loyale et transparente, ce qui signifie qu'il ne doit pas intervenir à l'insu de la personne concernée et/ou à des fins détournées. Les principes de **bonne foi** et de **reconnaissabilité** exigent que la collecte des données personnelles et, en particulier, les **finalités** du traitement, soient reconnaissables pour la personne concernée[19].
- Par ailleurs, le maître du fichier a une **obligation d'information** lorsqu'il collecte des données sensibles ou des profils de la personnalité la concernant[20].

Commentaire juridique
En application de cette **obligation d'information** qui incombe au maître du fichier, la personne concernée doit recevoir les informations suivantes : **identité** du maître du fichier; **finalités** du traitement pour lequel les données sont collectées; catégories de **destinataires** des données si la communication des données est envisagée (art. 14 al. 2); si les données ne sont **pas collectées auprès de la personne concernée**, celle-ci doit être informée au plus tard lors de leur enregistrement ou, en l'absence d'un enregistrement, lors de la première communication à un tiers (art. 14 al. 3); le maître du fichier est **délié de son devoir d'informer** si la personne concernée a déjà été informée; il n'est **pas non plus tenu d'informer** cette dernière dans les cas prévus à l'al. 3, si l'enregistrement ou la communication sont expressément prévus par la loi ou si le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés (art. 14 al. 4).

Recommandation pratique – évaluer la reconnaissabilité et obligation d'information
Pour chaque traitement de données personnelles, il y a lieu de vérifier si les exigences de transparence sont respectées (bonne foi, reconnaissabilité et éventuelle obligation d'information). En cas de doute, surtout lors du traitement de **données sensibles** ou de **profil de personnalité**, il est recommandé de s'adresser au département juridique, au département du Contrôle de Gestion, à la direction des technologies de l'information et, le cas échéant, au Conseiller à la Protection des Données.

5.3 Proportionnalité

- La **proportionnalité**[21] exige de ne traiter que les données nécessaires à réaliser le but recherché par ce traitement de données, de veiller à ce qu'il existe un rapport raisonnable entre ce but et le moyen utilisé, tout en préservant le plus possible les droits des personnes.

Commentaire juridique
Le principe de proportionnalité exige un traitement proportionné des données personnelles, ce qui signifie que ne doivent être traitées que les données **absolument nécessaires** à l'accomplissement du but recherché. L'exigence de proportionnalité vise notamment **la nature et la quantité** des données traitées, les **modalités de traitement et mesures de sécurité** appliquées, ainsi que la **durée de conservation**. Les **données sensibles** doivent faire l'objet d'une attention toute particulière. Les données devenues inutiles doivent en principe être **détruites ou anonymisées**, sauf si leur conservation avec possibilité d'identifier la personne concernée peut être justifiée par un droit et/ou une

[19] *Art. 4 al. 2 et 4 LPD.*
[20] *Art. 14 et art. 9 al. 1 et 4 LPD.*
[21] *Art. 4 al. 2 LPD.*

obligation de conservation, notamment à des fins d'archivage légal (voir également la directive ISMS 142 de conservation des documents et de l'information).

Recommandation pratique – identifier et retenir le traitement le moins invasif
Pour chaque traitement de données personnelles, il y a lieu de vérifier si l'exigence de proportionnalité est remplie (nature et quantité des données traitées, modalités de traitement et mesures de sécurité, durée de conservation). En particulier, il y a lieu de le restreindre le traitement à ce qui est strictement nécessaire et d'appliquer les modalités de traitement qui limitent le plus possible l'exposition de la sphère privée. Le **niveau de protection** des données peut être évalué en fonction de leur **degré de sensibilité**. En cas de doute, surtout en cas de collecte de **données sensibles** ou de **profil de personnalité**, il est recommandé de s'adresser au département juridique, au département du Contrôle de Gestion, à la direction des technologies de l'information et, le cas échéant, au Conseiller à la Protection des Données.

5.4 Finalité

- Le principe de **finalité** impose de ne traiter les données personnelles que dans le but indiqué lors de leur collecte[22], qui doit être déterminé préalablement à la collecte, et qui ne peut être modifié par la suite.

Recommandation pratique – consigner la finalité du traitement et veiller à son respect
Lors de la création d'un fichier de données personnelles, le maître du fichier doit décrire et consigner la finalité du traitement de données dans un document spécifique, concis et compréhensible par les personnes impliquées dans le traitement de données et par la personne concernée (notamment pour le cas où celle-ci demanderait à accéder à ses données[23]). Les modifications subséquentes de la finalité du traitement initialement prévue doivent pouvoir être reconstituées. Le maître du fichier doit veiller à ce que le traitement des données personnelles ne s'écarte pas du but défini, spécialement si le traitement porte sur des **données sensibles** ou sur des **profils de personnalité**. En cas de doute sur les mesures à prendre, surtout en cas de collecte de **données sensibles** ou de **profil de personnalité**, il est recommandé de s'adresser au département juridique, au département du Contrôle de Gestion, à la direction des technologies de l'information et, le cas échéant, au Conseiller à la Protection des Données.

5.5 Exactitude

- Le principe d'**exactitude** impose de s'assurer qu'elles sont correctes et de prendre toutes les mesures appropriées pour effacer ou rectifier des données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées[24]. Le corollaire du principe d'exactitude est notamment le droit pour la personne visée de requérir l'**accès** aux données traitées la concernant[25], ainsi que le droit de **rectifier** les données inexactes[26].

Recommandation pratique – veiller à la mise à jour et permettre la rectification
Lors de la collecte de données personnelles, le maître du fichier doit prendre les mesures raisonnables pour identifier la personne concernée par les données traitées et s'assurer de la validité et de la mise à jour des données collectées.

[22] *Art. 4 al. 3 LPD.*
[23] *Art. 8 LPD.*
[24] *Art. 5 al. 1 LPD.*
[25] *Le droit d'accès (art. 8 LPD) comporte notamment le droit de se voir indiquer le but et éventuellement la base juridique du traitement, les catégories de données personnelles traitées, de participants au fichier et de destinataires des données (art. 8 al. 2 let. b LPD).*
[26] *Art. 5 al. 2 LPD.*

5.6 Communication transfrontière de données

- Sauf communications pouvant présenter une menace grave pour l'intéressé, le transfert de données à l'étranger est en principe licite lorsque le pays de destination offre un niveau de protection adéquat[27].

Commentaire juridique
Le Préposé fédéral à la protection des données et à la transparence a notamment pour attribution d'examiner l'adéquation du niveau de protection assuré à l'étranger[28]. Il publie une liste des Etats qui disposent d'une législation assurant un niveau de protection adéquat[29]. L'Etat vers lequel les données sont transférées doit disposer d'une législation assurant un niveau de protection adéquat ; si tel n'est pas le cas, des garanties suffisantes, notamment contractuelles, doivent être prévues[30] ; à défaut, des conditions bien spécifiques doivent être remplies, notamment le consentement des personnes concernées[31].

Recommandation pratique – évaluer le risque juridique et les garanties nécessaires
En cas de projet impliquant un transfert de données à l'étranger, le maître du fichier doit s'adresser au département juridique, au département du Contrôle de Gestion ou à la direction des technologies de l'information pour s'informer des conditions à remplir et des précautions à observer, en particulier pour en évaluer et prévenir les risques, notamment par des garanties contractuelles.

5.7 Sécurité des données

- Le principe de **sécurité** exige de protéger les données par des mesures organisationnelles et techniques appropriées[32], pour prévenir les risques de destruction, erreurs, falsification, vol, modification, copie, accès ou autre traitement non autorisés[33]. Ces mesures doivent tenir compte du but du traitement, de la nature et étendue du traitement, d'une évaluation des risques potentiels pour les personnes concernées, des développements techniques[34].

Commentaire juridique
Afin d'assurer la **confidentialité des données**, il y a lieu de veiller à ce qu'elles ne soient pas communiquées ou révélées à des personnes non autorisées ; les mesures à prendre à cet effet concernent ou peuvent concerner[35] : la sécurité de l'information dans la gestion de projet, les appareils mobiles et le télétravail, la gestion des actifs, le contrôle d'accès, la cryptographie, la sécurité physique et environnementale, la journalisation et la surveillance, la gestion de la sécurité des réseaux, le transfert de l'information ; le **niveau de protection** des données peut être évalué en fonction de leur **degré de sensibilité**. Afin d'assurer l'**intégrité des données**, il y a notamment lieu de prévoir des protections contre les logiciels malveillants et d'assurer la maintenance des systèmes d'information. Afin d'assurer la **disponibilité des données**, il y a lieu de veiller à ce qu'elles soient accessibles et exploitables par les personnes autorisées, notamment en assurant la sauvegarde, l'enregistrement et la sécurité des informations et des systèmes d'information.

[27] *Art. 6 al. 1 LPD.*
[28] *Art. 31 al. 1 let. d LPD.*
[29] *Art. 7 OLPD.*
[30] *Art. 6 al. 2 let. a et g LPD.*
[31] *Art. 6 al. 2 let. b, c, d, e, f LPD.*
[32] *Art. 7 al. 1 LPD.*
[33] *Art. 8 OLPD.*
[34] *Art. 8 OLPD.*
[35] *Référence étant faite sur ce point à l'Annexe A d'ISO 27001, renvoyant intégralement à ISO 27002.*

Recommandation pratique – prendre les mesures organisationnelles et techniques
Pour toute question relative à la sécurité des données, notamment en ce qui concerne le degré de sensibilité des données traitées et des précautions à observer, il est recommandé de s'adresser en priorité au Département du Contrôle de Gestion, à la direction des technologies de l'information et au département juridique, le cas échéant au Conseiller à la Protection des Données.

5.8 Droit d'accès

- Toute personne peut demander au maître d'un fichier si des données la concernant sont traitées[36]. Le maître du fichier doit lui communiquer: toutes les données la concernant qui sont contenues dans le fichier, y compris les informations disponibles sur l'origine des données; le but et éventuellement la base juridique du traitement, les catégories de données personnelles traitées, de participants au fichier et de destinataires des données[37].

Commentaire juridique
Le maître du fichier qui fait traiter des données par un tiers demeure tenu de fournir les renseignements demandés. Cette obligation incombe toutefois au tiers, s'il ne révèle pas l'identité du maître du fichier ou si ce dernier n'a pas de domicile en Suisse[38]. A certaines conditions, le maître du fichier peut refuser ou restreindre la communication des renseignements demandés, voire en différer l'octroi[39].

Recommandation pratique – prendre toute mesure utile à respecter le droit d'accès
Les renseignements sont, en règle générale, fournis **gratuitement et par écrit**, sous forme d'imprimé ou de photocopie[40]. Le maître du fichier doit **organiser son fichier** de façon à permettre l'exercice du droit d'accès. A cet effet, il doit mettre en place les **outils de recherche** permettant de retrouver les données traitées et être en mesure de les soumettre à la personne concernée. Pour toute question relative au droit d'accès, il est recommandé de s'adresser au département juridique, au département du Contrôle de Gestion et, le cas échéant, au Conseiller à la Protection des Données.

6 Gestion des incidents

Les incidents liés à la protection des données personnelles doivent être traités en conformité avec la procédure ISMS 7 de gestion des incidents, qui prévoit ce qui suit :

- En cas d'événement, de situation ou d'incident indiquant la possibilité d'une violation des exigences légales et/ou des directives internes en matière de protection des données, les collaborateurs signalent immédiatement la situation au 888.
- Le directeur du département concerné, le Directeur du Contrôle de Gestion et le Directeur du département DOSI et, le cas échéant, le Conseiller à la Protection des Données, prennent les dispositions nécessaires pour identifier, analyser et remédier aux situations de non-conformité.
- La loterie Romande met en place une approche préventive pour éviter une nouvelle occurrence des incidents.

7 Documentation complémentaire

Les documents complémentaires suivants viennent appuyer cette politique :

- Politique ISMS 19 - Politique de sécurité de l'information de la Loterie Romande
- Procédure ISMS 7 - Gestion des incidents

[36] *Art. 8 al. 1 LPD.*
[37] *Art. 8 al. 2 let. a et b LPD.*
[38] *Art. 8 al. 3 LPD.*
[39] *Art. 9 LPD.*
[40] *Art. 8 al. 5 LPD.*

- Directive ISMS 142 de conservation des documents et de l'information
- Note interne - Principes généraux de la protection des données (08.12.14)
- Guide pratique – Directives et recommandations destinées aux collaborateurs impliqués dans le traitement des données personnelles
- Loi fédérale du 19 juin 1992 sur la protection des données (LPD)
- Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD)
- Ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données (OCPD)
- Disposition sur le Contrat de travail du Code des Obligations (CO), notamment l'article 328b CO
- Les articles 28 et suivants du Code Civil suisse (CC)
- Guide pour le traitement des données personnelles dans le secteur privé du Préposé fédéral à la protection des données
- Guide pour le traitement des données personnelles dans le secteur du travail / Traitement par des personnes privées du Préposé fédéral à la protection des données
- Guide relatif aux mesures techniques et organisationnelles de la protection des données du Préposé fédéral à la protection des données

8 Points de contrôle

Il est possible de consulter :

- les contrats liant la Loterie Romande à ses collaborateurs
- le règlement général des jeux de la Loterie Romande accessibles par Internet et par téléphone mobile.
- les clauses de confidentialité
- les autorisations d'accès aux données
- l'application GESPRIV afin de réviser les demandes et les attributions des droits d'accès.