الجامعة التونسيّة لشركات التأمين
Fédération Tunisienne des Sociétés d'Assurances

# Guide Pratique
## de Protection des Données Personnelles dans le Secteur des Assurances

**FTUSA**

**2023**

# PLAN

## Mot de la FTUSA

## Mot de M. Le Président de la FTUSA

**M. Hassène FEKI**

Dans le cadre de leur activité, les entreprises d'assurance et de réassurance sont amenées à recueillir d'importants volumes de données personnelles.
Ces informations, qui proviennent aussi bien des assurés eux-mêmes que des acteurs rencontrés pendant le parcours client , sont utilisées par ces entreprises afin de proposer des garanties réellement adaptées aux besoins des assurés.
La protection de ces données est donc essentielle.
Entre les entreprises d'assurances et leurs assurés, c'est une question à la fois de confiance et de respect de la loi.
Lors de la souscription d'un contrat d'assurances, les entreprises d'assurances et de réassurance recueillent de nombreuses données personnelles provenant essentiellement des formulaires à remplir dans le cadre du contrat (âge, sexe, domicile, profession, état de santé…) afin de mieux évaluer le risque et fixer les tarifs des contrats mais également des données nécessaires pour le règlement des sinistres.
Ces données étant confidentielles et parfois sensibles, leur utilisation est strictement encadrée : elles ne peuvent servir qu'à une finalité précise, annoncée en amont aux assurés, et pour une durée limitée, fixée par la loi.
Elles doivent être communiquées uniquement aux personnes et aux organismes intéressés et leur sécurité doit être garantie à tous les niveaux.
Ainsi, dans le cadre de l'assurance, la protection des données personnelles est déterminante.
Toutefois, c'est là que le bât blesse, car la protection des données personnelles dans l'assurance constitue un véritable défi réglementaire pour les assureurs.
Conscientes de ce défi majeur, les entreprises d'assurances et de réassurance adoptent des bonnes pratiques pour protéger les données des assurés telles que :

- La sensibilisation du personnel aux pratiques de gestion des données et de sécurisation des systèmes informatiques.
- La mise en place des processus internes inspirés de la loi sur la protection des données personnelles.
- Respect des délais de conservation des données.
- Sécurisation des accès des personnels et de toutes les personnes intéressées par la mise en place d'un système d'authentification forte dans le cadre de l'accès aux systèmes d'information.
- Stockage des données personnelles des assurés dans des serveurs sécurisés.
- Nomination d'un Data Protection Officer.

Certes, ces bonnes pratiques permettent de garantir la protection des données personnelles utilisées dans les entreprises d'assurances, mais la loi quel que soit son degré de détail, reste incapable d'apporter toutes les réponses aux problématiques quotidiennes rencontrées par les entreprises d'assurance. D'où l'idée de préparer un guide pratique de protection des données personnelles.
Durant plus d'une année l'équipe FTUSA et les DPO des entreprises d'assurances se sont penchés à l'élaboration d'un guide sectoriel afin de recenser ces problématiques et apporter des réponses communes tout en respectant la législation en vigueur.
Ce guide n'aurait jamais vu le jour sans l'implication de l'équipe de rédaction et bien évidement le concours et le soutien de l'INPDP et particulièrement de son Président le professeur Chawki GUEDDAS qui n'a épargné aucun effort pour orienter et appuyer cette équipe.
Merci à toutes les personnes qui ont contribué à la parution de ce guide.

## Mot du Directeur Général de la FTUSA
## M. Hatem AMIRA

Je suis ravi de vous informer de nos récents efforts dans la préparation d'un guide de protection des données personnelles. Cette initiative est une étape cruciale dans notre engagement à respecter la vie privée de nos assurés et à assurer la confidentialité de leurs informations.

Dans un monde de plus en plus connecté et numérique, la protection des données personnelles est devenue une préoccupation majeure pour les individus et les organisations.

En tant qu'acteurs clés du secteur de l'assurance, il est de notre responsabilité de veiller à ce que les données confidentielles de nos clients sont traitées de manière sécurisée et conformément aux lois et réglementations en vigueur.

Le guide de protection des données personnelles que nous avons élaboré vise à fournir des directives claires et pratiques pour nos Entreprises d'assurances afin de les aider à mettre en place des mesures adéquates de protection des données. Il aborde des sujets tels que la collecte et le stockage des données, l'accès restreint aux informations confidentielles, la sécurisation des réseaux et des systèmes, ainsi que les procédures en cas de violation de données.

La mise en place de ce guide est une démarche proactive de notre fédération pour améliorer les pratiques de protection des données dans l'ensemble du secteur de l'assurance en Tunisie. Nous encourageons tous nos DPO à prendre connaissance de ce guide et à le mettre en œuvre dans leurs activités quotidiennes.

En parallèle, nous travaillons également en étroite collaboration avec les autorités compétentes et les organismes de réglementation pour nous assurer que nos pratiques sont en conformité avec la législation en vigueur en matière de protection des données personnelles.

Nous souhaitons être à la pointe des dispositions règlementaires et des bonnes pratiques et contribuer activement à la mise en place d'un environnement de confiance pour nos assurés.

Ce guide comprend cinq chapitres et 9 annexes. Le premier chapitre définit tous acteurs du secteur de l'assurance au regard de la législation en vigueur en matière de protection des données à caractère personnel.

Le deuxième chapitre détaille les différentes données traitées dans le secteur des assurances.

Quant au troisième chapitre, il explique les différentes finalités en mentionnant à chaque fois la base légale de traitement.

Dans le quatrième chapitre, on trouve les obligations de l'assureur pour se conformer à la législation et règlementation en vigueur en matière de PDP. Ce chapitre aidera beaucoup les compagnies pour qu'elles soient en conformité et utiliser les bonnes pratiques.

Le cinquième et dernier chapitre explique les différents droits des personnes concernées tout en détaillant les délais, les cas de litige et les sanctions etc..

Je tiens à remercier M Chawki Guddes ainsi tous les DPO et l'équipe de rédaction pour leur engagement envers la préparation de ce guide pratique.

Notre objectif est le renforcement de la confiance de nos assurés et la garantie d'un avenir solide et durable pour le secteur de l'assurance en Tunisie.

## Mot du Président de l'INPDP
## M. Chaouki GUEDDES

Le domaine des assurances est un grand consommateur de données personnelles et c'est la mission qu'assure ces acteurs qui leur impose de collecter la plus grande masse de données sur leurs clients. Il est donc légitime pour les assureurs de collecter les données et de les traiter en vue d'analyser les risques ce qui leur permettra de les couvrir au profit de leurs clients.
Le développement des technologies de traitement des données crée de nouvelles pistes de collecte et de traitement des données personnelles. Ces avancées technologiques permettront de collecter des données sur la manière de conduire sa voiture automobile à travers un système GPS embarqué ou sur les activités physiques et sportives à travers des bracelets connectés que porteraient les clients. Mais les assureurs doivent collecter encore plus de données pour réduire les comportements frauduleux en recourant à différentes sources d'information et surtout à un échange de données entre les acteurs du secteur.
Ces traitements de plus en plus intrusifs dans la vie privée collectant de plus en plus des données sensibles des personnes concernées ne peux qu'inquiéter un protecteur des données personnelles. Il doit au cas par cas sans refuser systématiquement toute avancée technologique s'assurer que ce traitement est nécessaire et qu'il est accepté de manière éclairé et responsable par le client et par la suite si ces données sont traitées par la suite dans la limite de la finalité déclarée et en garantissant leur sécurisation.
Le respect des normes de protection des données personnelles est le meilleur garant pour les assureurs pour attirer les clients en leur assurant que leurs données seront traitées en toute confidentialité et que dans leur intérêt. La confiance est la notion clef de toute relation entre l'assureur et son client. Garantir la protection des données traitées est le meilleur garant pour pérenniser les rapports entre les deux parties.
Le secteur des assurances en Tunisie a été très vite conscient de cet impératif. Depuis 2016, différentes compagnies et à leur tête la FTUSA se sont rapprochées de l'INPDP pour demander à être accompagnées dans leur action de mise en conformité aux normes de protection des données personnelles.
Quand en 2020, l'INPDP a soumis comme dans d'autres secteurs d'activité les assureurs à des contrôles à distances, ils ont été les plus réactifs. Ils ont accepté de nommer en interne un chargé de la protection des données personnelles alors que la loi tunisienne ne l'imposait pas et se sont attelés à réaliser leur cartographie de traitement. Les assurances consultent souvent soit à travers des demandes d'avis ou informellement par téléphone l'INPDP sur la manière de faire à chaque fois qu'une situation nouvelle dans le traitement des données se présente à eux.
Ce guide élaboré par la FTUSA en collaboration avec des chargés de la protection des données de certaines assurances phare est la preuve de l'installation de la culture de la protection des données dans le secteur. Ce document de référence, que l'INPDP à cause de ces moyens humains limités ne pouvait élaborer pour les secteurs stratégiques comme les assurances, sera la bible de tout assureur qui voulant développer la confiance de ces clients dans son entreprise, y trouvera le mode d'emploi pour se mettre en conformité aux normes de protection des données personnelles.
L'INPDP est un contrôleur certes, mais c'est avant tout un accompagnateur des responsables de traitement et à ce titre elle ne peut que féliciter les acteurs du secteur et à leur tête la FTUSA en espérant que ce qu'ils réalisent aujourd'hui servira d'exemple à d'autres secteurs comme la banque ou le tourisme.

## Comité de Rédaction et de validation

• **M. Hatem AMIRA**, DG de la FTUSA
• **Mme Houda HAMDI**, Directeur Central à la FTUSA. Auparavant DPO et Responsable Audit Interne et Conformité au Lloyd Assurances et Lloyd Vie
• **Mme Mariem CHARFI**, DPO à la Star
• **Mme Sana HDIJI, DPO** DPO et responsable juridique et contentieux Assurances BIAT
• **M. Rachid BOURGUIBA**, DPO et RSSI COMAR et Hayett
• **M. Walid REBHI**, DPO et Responsable Conformité, Actuariat et Risk Management Assurances Maghrebia.
• **Mme Hiba MEJRI,** Cadre à la FTUSA

## Comité de validation

• **Comité Directeur de la FTUSA :** composé par tous les DG des entreprises d'assurances et de réassurance
• **Comité Exécutif de la FTUSA :** composé du Président de la FTUSA et des trois vice-présidents
• **Comité Permanent d'experts de la FTUSA des affaires économiques, sociales, juridiques, financières fiscales et de conformité**

## Comité élargi du projet d'élaboration du guide

Tous les chargés de protection de données personnelles et DPO du secteur des assurances

## Abréviations

PDP : Protection des Données personnelles
DP : Donnée personnelle
INPDP : Instance nationale de Protection des données personnelles
LBA/FT : Lutte contre le blanchiment d'argent et Financement du Terrorisme
FATCA: Foreign Account Tax Compliance
KYC: Know Your Costumer
PPE : Personne Politiquement exposée
FTUSA : Fédération Tunisienne des Sociétés d'assurance
CNLCT : Commission Nationale de Lutte contre le Terrorisme
CTAF : Commission Tunisienne des Analyses Financières
CGA : Comité Général des Assurances
RIB : Relevé d'identité Bancaire
IBAN: International Bank Account Number
Art.: Article
CIN : Carte d'identité NationaleISO : International Organisation for standardizations
VoIP : voie sur les protocoles internet
VPN : Virtual Private network
OTP : One Time Password/ mot de passe à usage unique
WPA2 : Wifi Protocol Access 2
WPA2-PSK : Wifi Protocol Access 2- Password Seva Kendras
SQL: Structured Query Language
TLS: Transport Layer Security
SSL: Secure Sockets Layer
IP: Internet Protocol
RAID: Redundant Array of Independent disks
SFTP : Secure File Transfer Protocol
OCDE : L'Organisation de coopération et de développement économiques
DPO : Data Protection officer
DG : Directeurs Généraux

# Lexique

**Adhérent**
Personne physique qui adhère à un contrat collectif souscrit par une personne morale ou un chef d'entreprise en sa dite qualité.

**Assuré** [1]
Personne dont la vie, les actes ou les biens sont garantis par un contrat d'assurance.
L'assuré n'est pas obligatoirement le souscripteur du contrat, ni le bénéficiaire de l'indemnité de l'assurance ni celui qui paie la prime.
Les contrats d'assurances précisent en général la définition de l'assuré.

**Auxiliaires et autres intervenants au contrat**
Il s'agit notamment des tiers payant, avocats, médecins, professionnels de santé et réseaux de soins, experts, enquêteurs, huissiers notaires, huissiers de justice liquidateurs, tuteurs, cautions, autres entités du groupe auquel appartient l'entreprise d'assurance ou le réassureur concerné, autres entreprises d'assurances concernées par le contrat d'assurance et les organismes de Sécurité Sociale.

**Ayant (s) droit**[2]
Le ou les membres de la famille (conjoint, ascendants et descendants) de la victime d'un dommage corporel lorsque celle-ci est décédée suite à un sinistre. Ils peuvent obtenir réparation de leurs préjudices (économique, moral etc…).

**Bénéficiaire du contrat d'assurance**[3]
Personne physique ou morale au profit de laquelle l'assurance a été contractée, c'est-à-dire qui reçoit les prestations prévues par le contrat en cas de réalisation du risque. Ce mot bénéficiaire est surtout utilisé pour les assurances sur la vie. Pour les autres assurances, celui qui reçoit l'indemnité est soit l'assuré, soit la « victime » en assurance de responsabilité civile.

**Coassurance**[4]
Opération par laquelle plusieurs assureurs couvrent un même risque, chaque assureur participant à hauteur d'un certain pourcentage.

**Comité Général des Assurances (CGA )**[5]

Comité doté de la personnalité morale et de l'autonomie financière. Son siège est à Tunis et il relève du ministère des finances. Il est l'autorité de contrôle du secteur des assurances.

[1] Site FTUSA : www.ftusanet.org
[2] Site FTUSA : www.ftusanet.org
[3] Site FTUSA : www.ftusanet.org
[4] Site FTUSA : www.ftusanet.org
[5] Site CGA : www.cga.gov.tn et article 177 du code des assurances

**Expert**[6]
Tout prestataire de service habilité à rechercher les causes, la nature, l'étendue des dommages et leur évaluation. Sa mission est exclusivement technique.

**Fédération Tunisienne des Sociétés d'Assurances (FTUSA)**[7]
Association professionnelle des entreprises d'assurances. A ce jour, ses membres adhérents sont 24 entreprises d'assurances et de réassurances de droit tunisien agrées à pratiquer les opérations d'assurances. Elle est habilitée à soumettre à l'autorité de tutelle toute question intéressant l'ensemble de la profession.

**L'Instance Nationale de la Protection des Données à caractère Personnel (INPDP)**
Autorité administrative indépendante qui a pour mission d'installer la culture de la protection, veiller au respect des normes de protection des données personnelles par les responsables de traitement et accompagner les personnes concernées dans l'exercice de leurs droits.

**Intermédiaire**
Toute personne physique ou morale autre qu'une entreprise d'assurance ou de réassurance qui, contre rémunération, présente par son entremise les opérations d'assurances au public. Les intermédiaires sont fixés par l'article 69 du code des assurances et qui sont à ce jour les suivants :

- **L'agent d'assurances :** La personne chargée en vertu d'un mandat de conclure des contrats d'assurances au nom et pour le compte d'une ou plusieurs entreprises d'assurances. Il exerce individuellement ou dans le cadre d'une société civile professionnelle.
- **Le courtier d'assurances** : La personne mettant en rapport des preneurs d'assurances et des entreprises d'assurances ou de réassurances sans être tenu dans le choix de celle-ci à l'effet d'assurer ou de réassurer des risques. Le courtier est le mandataire de l'assuré et est responsable envers lui.
- **Le producteur en assurance sur la vie :** La personne physique salariée ou non, mandatée par une entreprise pratiquant les opérations d'assurances sur la vie. L'activité du producteur est limitée à la présentation des contrats et éventuellement à l'encaissement des primes. Le producteur en assurance sur la vie ne peut représenter qu'une entreprise d'assurance.
- **Les banques :** chargées en vertu d'une convention de conclure des contrats d'assurances au nom et pour le compte d'une ou de plusieurs entreprises d'assurances, quelle que soit sa forme et nonobstant toutes dispositions contraires, et ce, pour les branches d'assurances dont la liste est fixée par un arrêté du Ministre des Finances.
- **L'Office National des Postes :** chargé en vertu d'une convention de conclure des contrats d'assurances au nom et pour le compte d'une ou de plusieurs entreprises d'assurances, et nonobstant toutes dispositions contraires, et ce, pour les branches d'assurances dont la liste est fixée par un arrêté du Ministre des Finances.
- **Les institutions de microfinance :** chargées, en vertu d'une convention, de conclure des contrats d'assurances au nom et pour le compte d'une ou de plusieurs entreprises d'assurances, quelle que soit sa forme et nonobstant toutes dispositions contraires, et ce, pour les branches d'assurances dont la liste est fixée par un arrêté du Ministre des Finances.

Il est à noter que la liste pourrait être élargie suivant la règlementation et législation en vigueur future

[6] Article 79 du code d'assurances
[7] Site CGA : www.cga.gov.tn et l'article 91 du code des assurances

**Souscripteur**[8]

Personne physique ou morale qui en signant le contrat d'assurances s'engage pour elle-même et pour les assurés aux Conditions Générales et Particulières de ce contrat.

**Réassurance**[9]

Sont considérées comme entreprises spécialisées en réassurances, les entreprises qui se livrent exclusivement, à titre d'activité habituelle, aux opérations d'acceptation et de cession des risques et ne pratiquant pas la souscription et l'exécution des contrats d'assurances.

[8] Site FTUSA : www.ftusanet.org
[9] L'article 48 du code des assurances.

## Liste des annexes[10]

**Annexe 1 :** Clause type de Protection des données personnelles du sous-traitant
**Annexe 2 :** Modèle de mention d'informations
**Annexe 3 :** Engagement de confidentialité
**Annexe 4** : Modèle du formulaire d'exercice des droits de Protection des données personnelles
**Annexe 5 :** Fiche de cartographie modèle de l'INPDP
**Annexe 6 :** Registre de traitements modèle de base de l'INPDP
**Annexe 7 :** Charte/politique de Protection des données personnelles
**Annexe 8 :** Conditions générales d'utilisation du site web
**Annexe 9 :** Recueil des textes en rapport avec la Protection des données personnelles

[10] Les annexes sont élaborées à titre indicatif

# CHAPITRE 1

# QUALIFICATION DES ACTEURS DU SECTEUR DE L'ASSURANCE AU REGARD DE LA LEGISLATION EN VIGUEUR EN MATIERE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

## 1. Les intervenants prévus par la législation en vigueur

**Responsable du traitement :** Toute personne physique ou morale qui détermine les finalités et les moyens du traitement des données à caractère personnel.

**Sous-traitant :** Toute personne physique ou morale qui traite des données à caractère personnel pour le compte et sous le contrôle du responsable du traitement.

**Tiers :** Toute personne physique ou morale ou l'autorité publique ainsi que leurs subordonnés, à l'exception de la personne concernée, le bénéficiaire, le responsable du traitement, le sous-traitant ainsi que leurs subordonnés.

**Bénéficiaire :** Toute personne physique ou morale recevant des données à caractère personnel.
Personne concernée :Toute personne physique dont les données à caractère personnel font l'objet d'un traitement.

**Personne concernée** [11]
Toute personne physique dont les données à caractère personnel font l'objet d'un traitement.

## 2. Définition des relations entre les intervenants

| L'entreprise d'assurance et l'assuré | |
|---|---|
| **Type de Relation** | Contrat d'assurance: l'un des documents du contrat d'assurance doit comporter une clause de protection des données personnelles tels que les conditions générales ou les conditions particulières/bulletin d'adhésion ou fiche KYC à condition que ce document soit signé par le souscripteur/l'adhérent (cf. Modèle de mention d'informations annexe 2)<br>Si le souscripteur est différent de l'assuré ou le/les bénéficiaire(s), la signature du souscripteur fait foi. |
| **Traitement nécessitant des données personnelles** | Ensemble des traitements répondant aux finalités de gestion des contrats d'assurances (incluant la souscription, l'exécution des garanties du contrat, la lutte contre la fraude, la LBA/FT, les études actuarielles etc…) |
| **Détermination des finalités** | Par l'entreprise d'assurance |
| **Détermination des moyens de traitement** | Par l'entreprise d'assurance |
| **Degré de responsabilité** | Responsabilité de l'entreprise d'assurance |
| **Conclusion**<br>**L'entreprise d'assurance est le responsable du traitement et l'assuré est la personne concernée** | |

[11] La personne physique représentant la personne morale est aussi considérée comme «personne concernée»

| L'entreprise d'assurance et l'intermédiaire en assurance | |
|---|---|
| **Type de Relation** | Convention comportant une clause de protection des données personnelles ou un engagement de protection des données personnelles signé par l'intermédiaire en assurance ou en réassurance (cf. Clause type de Protection des données personnelles du sous-traitant : annexe 1) |
| **Traitement nécessitant des données personnelles** | Ensemble des traitements répondant aux finalités de prospection commerciale dans le cadre du mandat y compris par l'utilisation du fichier de portefeuille de clients qui lui est confié par l'entreprise d'assurances,<br><br>Ensemble des traitements répondant aux finalités de gestion des contrats d'assurances dans le cadre du mandat. |
| **Détermination des finalités** | Par l'entreprise d'assurance |
| **Détermination des moyens de traitement** | Par l'entreprise d'assurance |
| **Degré de responsabilité** | Par l'entreprise d'assurance |

**Conclusion**
**L'entreprise d'assurances est le responsable du traitement et l'intermédiaire est le sous-traitant**

| Les entreprises d'assurance entre elles | |
|---|---|
| **Type de Relation** | Contrat d'assurances en coassurance ou Convention inter-compagnies (sectorielles élaborées dans le cadre de la FTUSA) comportant une clause de protection des données personnelles ou un engagement de protection des données personnelles signé par les parties contractantes (cf. Clause type de Protection des données personnelles du sous-traitant : annexe 1) |
| **Traitement nécessitant des données personnelles** | Traitements répondant aux finalités de gestion des contrats d'assurances |
| **Détermination des finalités** | Par chacune des entreprises d'assurance indépendamment des autres |
| **Détermination des moyens de traitement** | Par chacune des entreprises d'assurance indépendamment des autres |
| **Degré de responsabilité** | Par chacune des entreprises d'assurance indépendamment des autres |

**Conclusion**
**Chaque entreprise d'assurance est responsable du traitement effectué**

## L'entreprise d'assurance et l'auxiliaire ou le prestataire de services

| | |
|---|---|
| **Type de Relation** | Convention comportant clause de protection des données personnelles ou un engagement de protection des données personnelles signé par le sous-traitant (cf. Clause type de Protection des données personnelles du sous-traitant : annexe 1). |
| **Traitement nécessitant des données personnelles** | Exécution des prestations |
| **Détermination des finalités** | Par l'entreprise d'assurance |
| **Détermination des moyens de traitement** | Par l'entreprise d'assurance |
| **Degré de responsabilité** | Responsabilité de l'entreprise d'assurance |

**Conclusion**
**L'entreprise d'assurance est le responsable du traitement**
**Et les autres acteurs sont des sous-traitants**

## L'entreprise d'assurance et le réassureur

| | |
|---|---|
| **Type de Relation** | Traité de réassurance ou tout autre document contractuel comportant une clause de protection des données personnelles ou un engagement de protection des données personnelles signé par le réassureur (cf. Clause type de Protection des données personnelles du sous-traitant : annexe1) |
| **Traitement nécessitant des données personnelles** | Gestion de la réassurance |
| **Détermination des finalités** | Par le réassureur et par l'entreprise d'assurance |
| **Détermination des moyens de traitement** | Par le réassureur et par l'entreprise d'assurance |
| **Degré de responsabilité** | Par le réassureur et par l'entreprise d'assurance |

**Conclusion**
**Chacun est responsable de son propre traitement**

| L'entreprise d'assurance et les autorités publiques | |
|---|---|
| **Type de Relation** | La relation est régie par la législation en vigueur et les données personnelles sont transmises sur la base d'une obligation légale |
| **Traitement nécessitant des données personnelles** | Exercice des missions déterminées par la législation en vigueur |
| **Détermination des finalités** | Par l'entreprise d'assurance |
| **Détermination des moyens de traitement** | Par l'entreprise d'assurance |
| **Degré de responsabilité** | Responsabilité de l'entreprise d'assurance |

**Conclusion**
**L'entreprise d'assurance est le responsable du traitement**

| L'entreprise d'assurance et la FTUSA | |
|---|---|
| **Type de Relation** | Conventions sectorielles comportant une clause de protection des données personnelles signées par les parties contractantes (cf. Clause type de Protection des données personnelles du sous-traitant : annexe 1). |
| **Traitement nécessitant des données personnelles** | Echange des données personnelles dans le cadre des conventions sectorielles |
| **Détermination des finalités** | La FTUSA |
| **Détermination des moyens de traitement** | La FTUSA |
| **Degré de responsabilité** | La FTUSA et les entreprises d'assurance |

**Conclusion**
**Chacun est responsable de son propre traitement**

# CHAPITRE 2

# LES CATEGORIES DE DONNEES A CARACTERE PERSONNEL

Dans le cadre de l'activité d'assurance et de réassurance, les entreprises d'assurances peuvent collecter des données personnelles de différentes catégories. Celles-ci sont traitées uniquement pour des finalités déterminées, explicites et légitimes.
Ainsi, les principales catégories de données traitées sont les suivantes :

## 1. Les données d'identification:

Les données relatives à l'identification des personnes, parties intéressées ou intervenantes au contrat sont notamment :

- Les noms et prénoms,
- La date et le lieu de naissance,
- La nationalité,
- La photo,
- Les numéros des pièces d'identité,
- Le numéro de sécurité sociale,
- L'adresse IP et toutes autres données de sources internes ou externes permettant d'identifier la personne.

## 2. Les données relatives à la situation familiale:

La situation familiale comprend notamment les éléments relatifs à :

- La situation matrimoniale (marié(e), veuf (ve), divorcé (e)),
- La composition du foyer (nombre d'enfant, âge…),
- Les personnes à charge (Ascendant et descendant, …),
- Les héritiers,
- Les bénéficiaires.

## 3. Les données relatives à la situation économique, patrimoniale et financière :

Les données relatives à la situation économique, financière et patrimoniale sont notamment les éléments relatifs aux :

- Salaire,
- Patrimoine mobilier et immobilier,
- Les autres revenus,
- Crédit,
- Les remboursements de crédit,
- Les intérêts des crédits,
- Données fiscales telles que l'identifiant fiscal, le régime fiscal, le statut fiscal, le pays de résidence et l'imposition.

## 4. Les données relatives à la situation professionnelle :

Les données relatives à la situation professionnelles sont notamment :

- La catégorie socioprofessionnelle,
- Le domaine d'activité,

- La profession,
- L'employeur,
- Les catégories de personnels assurés,
- La convention collective,
- La date prévisionnelle de départ à la retraite,
- Le régime fiscal,
- Les compétences et qualifications professionnelles,
- Les diplômes et formations,
- Le grade et la fonction,
- Les justificatifs de demandeur d'emploi…

## 5. Les données de géolocalisation des personnes ou des biens en relation avec les risques assurés ou les services proposés

Ces données sont notamment :

- Les adresses postales,
- Les adresses électroniques,
- Les contacts téléphoniques,
- La position du véhicule assuré lorsque cela entre dans les conditions de mise en œuvre du contrat d'assurance.

## 6. Les données relatives aux habitudes de vie et aux usages des biens en relation avec les risques assurés ou les services proposés

Les données relatives aux habitudes de vie en relation avec les risques assurés ou les services proposés sont :

- Les loisirs,
- Les activités sportives et de plein air,
- La pratique de la chasse, de la plaisance,
- Les trajets,
- Les kilométrages parcourus

Les données relatives aux usages des biens en relation avec les risques assurés ou les services proposés sont notamment les données nécessaires pour les contrats d'assurance véhicule professionnel, personnel, résidence principale et résidence secondaire, présence d'animaux domestiques.

## 7. Les données relatives à la détermination ou à l'évaluation des préjudices et des prestations

Il s'agit notamment :

- Des données liées au sinistre : la nature et les circonstances du sinistre, la description des atteintes aux biens et/ou aux personnes, les Procès-verbaux de police et autres rapports d'enquête, les rapports d'expertise, les éléments afférents aux procédures administratives ou judiciaires éventuellement engagées ;
- Des données liées aux victimes : la nature et l'étendue des préjudices subis, le taux d'invalidité / d'incapacité, les rentes, le capital décès, les montants des prestations, les modalités de

règlement, la réversion, les montants remboursés par la sécurité sociale pour les complémentaires frais de soins (maladie, maternité) ;

## 8. Les données sur les risques clients ou de la transaction

Les données sur les risques clients ou de la transaction sont :

- Données sur la solvabilité et les données relatives aux actions collectives dont les jugements de faillite,
- Données relatives à l'implication ou la suspicion dans des actes et/ou transactions frauduleux,
- Données relatives aux déclarations et prestations sur sinistres d'assurance et données sur le risque d'impayé et le recouvrement des créances,
- Données relatives à l'application des règles relatives à la lutte contre le blanchiment d'argent et le financement du terrorisme et toutes informations liées aux contrôles requis par la législation en vigueur pour la gouvernance des risques.
- Numéro de chèque ;
- Numéro de carte bancaire et sa date de fin de validité.
- Les références bancaires (RIB / IBAN).
- Données mentionnées au niveau du formulaire de déclaration du risque (FDR) et autres formulaires

## 9. Les données sur les services demandés ou utilisés et comportement liés à ces services :

Il s'agit notamment :

- Des données contenues dans la documentation client ou dans les formulaires de l'assureur,
- Des données sur les services demandés, en cours d'utilisation ou utilisés dans le passé notamment les garanties incluses dans les contrats d'assurances et les sinistres déclarés,
- Données sur les canaux de distribution,
- Données relatives aux habitudes et aux préférences par rapports aux services offerts.

## 10. Les données sur les interactions

Ce sont les données relatives aux interactions avec les Intermédiaires en assurances, sur les sites Internet, sur les applications et les courriers postaux et/ou électroniques et par tout autre moyen de communication notamment pour demander un service ou une assistance, faire une réclamation ou en répondant à une enquête de satisfaction.

## 11. Les données sensibles

Les données personnelles sont de deux types, celles ordinaires ou classiques mais aussi celles considérées comme sensibles qui doivent faire l'objet d'une attention toute particulière de la part des responsables de traitement.
Les données sensibles sont des données à caractère personnel qui contiennent des informations sensibles qui, si elles étaient révélées, pourraient avoir des incidences néfastes sur la vie privée des personnes concernées ou dont le traitement est susceptible de leur créer des risques.

Qui peuvent entrainer des discriminations à l'égard des personnes concernées ou qui portent sur des données d'identification physique.

Selon la législation en vigueur en matière de protection des données à caractère personnel et selon les règles de conduite de l'INPDP, les données sensibles sont celles qui concernent directement ou indirectement :

- L'origine raciale ou ethnique
- Les convictions religieuses, les opinions politiques, philosophiques ou syndicales
- Les données relatives à l'orientation sexuelle et plus largement à la vie sexuelle
- Les données de santé : état et historique de santé : Ce sont les données sur la santé requises pour la conclusion de contrats d'assurance ou le règlement de prestations en cas de maladie, d'incapacité, d'invalidité ou de décès.

Elles sont les données sur la santé requises pour la conclusion de contrats d'assurance ou le règlement de prestations en cas de maladie, d'incapacité, d'invalidité ou de décès.
Les chargés de la souscription et de la gestion des contrats d'assurances et les gestionnaires des indemnisations de quelques branches d'assurance traitent des données santé dans l'exécution de leurs missions.  Toutefois, ils doivent signer un engagement de confidentialité (cf annexe 3)
Il est à préciser que les plis fermés comportant des lettres confidentielles ou autres concernant le dossier médical sont traités directement par les médecins conventionnés des entreprises d'assurances.

- Les données biométriques permettant d'identifier une personne de manière unique (les empreintes par exemple)
- Les données génétiques
- Les données pénales : les infractions commises et les condamnations
- Les données de localisation : l'utilisation d'une technique permettant de déterminer le lieu où se trouve la personne concernée par le traitement,
- La vidéosurveillance

# CHAPITRE 3

# LES FINALITES[12] ET LES BASES LEGALES

[12] Les finalités concernent le volet métier des assurances et de réassurance. Les autres finalités des activités support seront développés dans la prochaine version de ce guide.

# 1. La gestion commerciale précontractuelle: La prospection commerciale

## A. Base légale : Nécessaire à l'activité / intérêt légitime

### *a. Prospection destinée à un Particulier :*

- Par voie postale[13] ou appels téléphoniques
- Par voie électronique pour les clients de la compagnie d'assurances

### *a. Prospection destinée à un professionnel :*

Trois principales étapes :

- Sélection des prospects,
- Choix des moyens de prospection,
- Réalisation de la prospection

Objectifs des opérations avec les prospects :

- Fidélisation
- Prospection
- Sondage
- Test des produits ou services existants
- Test de nouveaux produits ou services
- Promotion
- Parrainage
- Jeux concours
- Opérations de sollicitations
- Statistiques commerciales

## B. Base légale: consentement

### *a. Transfert des données à l'étranger*

Il s'agit du transfert des données personnelles des prospects à l'étranger généralement soit à des réassureurs, courtiers ou des sous-traitants

### *b. Prospection destinée à un Particulier client potentiel par voie électronique.*

Les étapes et les objectifs sont les mêmes que ceux cités ci-dessus (Ref : étapes et objectifs des opérations avec les prospects).

[13] En cas de prospection par voie postale, l'entreprise d'assurance doit insérer la possibilité de s'opposer et à travers quel moyen.

# 2. La gestion commerciale contractuelle

## A. Base légale : Nécessaire à l'activité / intérêt légitime

### *a. La Fidélisation des clients, l'amélioration de la qualité de service et les opérations promotionnelles*

Il s'agit des traitements relatifs :

- Aux programmes de fidélité ou aux jeux concours ;
- A la connaissance des attentes des clients ou à la réalisation d'enquêtes de satisfaction.

### *b. Effectuer des statistiques*

La direction commerciale pourrait effectuer des statistiques commerciales et traiter par conséquent les données personnelles des clients.

### *c. Animation du réseau*

- **La gestion et l'animation du réseau**
  - Participer à la définition de la stratégie d'implantation ou de développement du réseau, à la sélection de ses membres ou au pilotage de son déploiement,
  - Organiser le fonctionnement du réseau (modalités de reporting, gestion des moyens alloués et des budgets commerciaux…),
  - Apporter un soutien technique et commercial au réseau, et notamment aux intermédiaires non-salariés dans la gestion de leur portefeuille,
  - Assurer, le cas échéant, la gestion intérimaire d'une agence d'assurance,
  - Animer, informer et former le réseau commercial.

- **Le développement commercial**
  - Concevoir, mettre en œuvre ou coordonner des plans d'actions commerciales,
  - Définir ou négocier les objectifs de vente ou de prescription, individuels ou collectifs,
  - Elaborer et mettre à jour des tableaux de suivi de l'activité et des résultats commerciaux du réseau,
  - Opérer des contrôles de qualité et de conformité sur le travail réalisé par le réseau,

- **Le conseil, l'accompagnement et l'aide à la décision**
  - Soutenir, stimuler, fédérer et fidéliser le réseau.
  - Organiser l'échange de bonnes pratiques et du savoir-faire au sein du réseau.

# 3. Le métier de l'assurance et de la réassurance : La gestion et l'exécution du contrat d'assurance

## A. Base légale : Exécution d'un contrat

### *a. La souscription et la gestion des contrats*

Il s'agit du traitement des données personnelles ordinaires et sensibles[14] nécessaires à la souscription et la gestion des contrats en direct ou en ligne et ce dans le cadre de la préparation et l'octroi des documents précontractuels et contractuels, des opérations relatives au règlement des primes ou cotisations et de l'établissement et la conservation des documents comptables y afférents, des modifications subséquentes de garantie en cours de contrat amenant à la préparation d'avenants, des opérations de répartition éventuelle entre les coassureurs et les réassureurs, du commissionnement, de la surveillance des risques, et des autres opérations techniques.

### *b. L'exécution des garanties des contrats*

Il s'agit du traitement des données personnelles ordinaires et sensibles[15] nécessaires à la mise en œuvre des garanties et des prestations (évaluation des dommages et/ou préjudices et calcul et versement du montant de l'indemnisation). Dans ce cadre, les données collectées sont relatives à la gestion des prestations, à la gestion des sinistres et à la gestion des transferts.

### *c. L'exercice des recours*

L'exercice des recours correspond notamment aux situations où l'assureur qui a indemnisé son assuré, se retrouve subrogé dans ses droits et peut alors se retourner contre le responsable du dommage.

### *d. L'élaboration des statistiques et des études actuarielles*

Le traitement des données personnelles se fait lors de l'élaboration des statistiques et études actuarielles et ce, dans le but de la tarification et la surveillance du portefeuille et afin de justifier que les engagements contractuels sont compatibles avec la solvabilité.

### *e. La perfection des produits (conduite d'activité…)*

Il s'agit notamment des traitements qui visent à améliorer des produits et services.
Il ne s'agit pas de modifier les garanties contractuelles des assurés mais plutôt de proposer par exemple des améliorations concernant les processus de gestion des contrats.

### *f. La réassurance*

Il s'agit du traitement des données personnelles par la structure Réassurance au sein de l'entreprise d'assurances. Les données personnelles sont transférées par cette dernière aux réassureurs qui sont en quasi-totalité hors du territoire tunisien (une autorisation auprès de l'INPDP est nécessaire puisqu'il s'agit d'un transfert à l'étranger).

[14] Les données de santé, les données génétiques, , les données de géolocalisation : l'utilisation d'une technique permettant de déterminer le lieu où se trouve la personne concernée par le traitement.
[15] Les données de santé, les données pénales (les infractions commises et les condamnations), les données de localisation : l'utilisation d'une technique permettant de déterminer le lieu où se trouve la personne concernée par le traitement.

### g. La coassurance

Il s'agit des traitements des données personnelles effectués dans le cadre d'un partage de couverture des risques assurantiels par plusieurs compagnies d'assurances (apériteur et coassureurs) à hauteur d'un certain pourcentage.

### h. Le recouvrement amiable et contentieux

Il s'agit notamment des traitements qui visent à recouvrir les primes d'assurances impayées par la voie amiable et contentieuse.
Le traitement se fait par les départements internes (précontentieux et contentieux) et externes tels que les huissiers notaires, les avocats et les sociétés de recouvrement.

### i. La lutte contre la fraude

La fraude peut être définie comme étant un acte commis intentionnellement par une ou plusieurs personnes physiques ou morales pour réaliser un avantage ou un bénéfice de façon illégale.
Ainsi, elle peut revêtir un caractère pénal (ex : escroquerie) ou civil (ex : faute intentionnelle ou dolosive de l'assuré).

Elle peut concerner la phase de souscription ainsi que la phase de gestion des sinistres.
Le traitement de lutte contre la fraude est consubstantiel à la gestion de l'exécution des contrats.
Ces traitements permettent de prévenir, de détecter ou de gérer les opérations, actes, ou omissions présentant un risque de fraude et émanant soit :

- pour la fraude externe : des personnes intéressées ou intervenant au contrat ;
- pour la fraude interne : des personnels salariés, des prestataires, des agents d'assurances, des mandataires, des intermédiaires, des administrateurs, mandataires sociaux, ou des élus des organismes.

### j. La sous-traitance

La sous-traitance est définie par tout appel à des tiers pour l'exercice d'activités ou de processus qui sont propres à l'entreprise d'assurance et exercés de manière récurrente ou continue.
Lors de la sous-traitance, la compagnie d'assurances est amenée à transférer les données personnelles des assurés et personnes concernées pour traitement.
En contrepartie, le sous-traitant doit respecter les exigences légales et règlementaires en matière de Protection des données personnelles.

## B. Base légale : Obligation légale

Il s'agit à titre d'exemple du traitement des données personnelles dans le cadre de la lutte contre le blanchiment des capitaux et le financement du terrorisme, des conventions FATCA et avec l'OCDE, du respect des sanctions économiques et financières internationales, circulaires et décisions du CGA.
Ainsi, il s'agit également du traitement des données qui sont nécessaires à l'exercice des missions confiées aux autorités publiques dans le cadre de la sécurité publique ou de la défense nationale, ou qui s'avèrent nécessaires à la mise en œuvre des poursuites pénales ou à l'exécution des missions dont elles sont investies conformément aux lois et règlements en vigueur[16] .

[16] Article 47 de la loi organique n°63 du 27 juillet 2004.

Nous développons ci-dessous à titre d'exemple, la Lutte contre le blanchiment d'argent et le Financement du Terrorisme et la fonction actuarielle :

### *a. La lutte contre le blanchiment d'argent et le Financement du Terrorisme*

Il s'agit des traitements des données personnelles des souscripteurs, assurés et bénéficiaires des contrats d'assurances dans le cadre de l'application de la législation et la réglementation en vigueur relative à la lutte contre le blanchiment d'argent et le financement du terrorisme[17] . Ainsi, il s'agit principalement des traitements afin de :

1 - La mise en œuvre des obligations de vigilance à l'égard de la clientèle conformément à l'approche par les risques;

2 - La recherche des personnes qui doivent faire l'objet de mesures de vigilance complémentaires en tant que personnes politiquement exposées (PPE);

3 - Le déclenchement des alertes et déclarations de soupçon ;

4 - La mise sous surveillance de certains contrats ou clients sur la base de la classification des risques élaborée par la compagnie, ou d'opérations jugées complexes, d'un montant inhabituellement élevé ou ne paraissant pas avoir de justification économique ou d'objet licite, ou d'une déclaration de soupçon n'ayant pas donné lieu à la résiliation de contrat;

5 - L'Analyse et la détermination du niveau de risque propre à chaque opération de maniement des fonds ;

6 - La mise en place d'une surveillance adaptée visant à détecter les opérations portant sur des sommes dont elle sait, soupçonne ou a de bonnes raisons de soupçonner qu'elles proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an ou participent au financement du terrorisme ;

7 - La garantie du respect des éventuelles mesures relatives aux sanctions financières nationales et internationales d'embargo et de gel des avoirs en vigueur ;

8 - Les vérifications complémentaires nécessaires;

9 - L'application des mesures de gel des avoirs.

### *b.La fonction actuarielle*

La fonction actuarielle est une fonction clé de gouvernance nécessaire pour une entreprise d'assurance et de réassurance et ce, suite à la Décision CGA n°01/2016 du 13 Juillet 2016[18].

**Ainsi, la fonction actuarielle traite les données personnelles en vue de :**

- Coordonner le calcul des provisions techniques, garantir le caractère approprié des méthodes, des modèles sous-jacents et des hypothèses utilisées
- Apprécier la suffisance et la qualité des données utilisées dans le calcul des provisions techniques ;
- Emettre un avis sur la politique globale de souscription ;
- Emettre un avis sur l'adéquation des dispositions prises en matière de réassurance ;
- Informer l'organe d'administration ou de gestion de la fiabilité et du caractère adéquat du calcul des provisions techniques ;

[17] conformément à la loi organique N°2015-26 du 07 août 2015 modifiée par la loi organique N°2019-9 du 23 Janvier 2019 , au décret gouvernemental n°2019-419 du 17 mai 2019 relatif aux procédures de mise en œuvre des résolutions prises par les instances onusiennes compétentes liées à la répression du financement du terrorisme et de la prolifération des armes de destruction massive, tel que modifié par le décret gouvernemental n°2019-457 du 31 mai 2019 et au règlement n°2 du 28 Aout 2019 relatif aux mesures de vigilance requises en matière de Lutte contre le Financement du Terrorisme et de prolifération des armes et la répression du blanchiment d'argent dans le secteur des assurances.

[18] Fixant les règles de la bonne gouvernance et de gestion dans les sociétés d'assurance et de réassurance.

## 4. Le profilage et le traitement automatisé

Le profilage est défini[19] comme : «Toute forme de traitement automatisé de données à caractère personnel visant à évaluer certains aspects personnels d'une personne physique et ayant pour finalité la connaissance de ses spécificités, ses préférences, ses choix, ses comportements d'une manière affectant son statut juridique.»
Pour mettre en œuvre les finalités citées ci-dessus, les responsables de traitement peuvent avoir recours au profilage tel qu'il est défini.
Le profilage est un moyen à disposition des Entreprises d'assurance et de Réassurance dans le cadre de la finalité gestion et exécution des contrats d'assurance pour évaluer les caractéristiques du risque assurantiel et en déterminer la fréquence, le coût moyen, le coût du sinistre maximum possible, la tarification et vérifier l'assurabilité du risque.

Le profilage peut également être utilisé, à titre d'exemples, dans le cadre de la LBA/FT, la FATCA, de la gestion des Ressources humaines, de la surveillance du portefeuille, des actions commerciales, de l'attribution des droits d'accès par les utilisateurs des Systèmes d'information, etc…

Lorsque l'entreprise d'assurance et de réassurance a recours au profilage, elle doit en indiquer l'existence dans les mentions d'information afin de permettre aux personnes concernées de comprendre la finalité exacte du profilage et l'usage qui est fait de leurs données,
La personne concernée par le traitement a le droit de s'opposer au profilage et aux effets juridiques qui s'en produisent, à moins que le traitement ne soit nécessaire pour l'exécution
d'une obligation juridique ou contractuelle[20]

[19] Art. 4 du Projet de loi organique n° 25/2018 relatif à la protection des données à caractère personnel
[20] Art. 74 du Projet de loi organique n° 25/2018 relatif à la protection des données à caractère personnel

# CHAPITRE 4

# LES OBLIGATIONS DE L'ASSUREUR

# 1.La cartographie et le registre de traitements

## A. La cartographie

La cartographie est l'étape indispensable à la réalisation du registre des traitements, exigées par l'Instance nationale de protection des données personnelles de Tunisie (INPDP). Il est donc crucial que cette technique soit maîtrisée.

De ce fait, il est utile de donner des réponses aux questions suivantes :

### *QUI ?*

Inscrivez dans le registre le nom et les coordonnées du responsable du traitement (et de son représentant légal) et, le cas échéant, du délégué à la protection des données ;
Identifiez les responsables des services opérationnels traitant les données au sein de votre organisme ;
Etablissez la liste des sous-traitants.

### *QUOI ?*

Identifiez les catégories de données personnelles traitées
Identifiez les données sensibles

### *POURQUOI ?*

Indiquez-la ou les finalités pour lesquelles vous collectez ou traitez ces données personnelles.

### *OÙ ?*

Déterminez le lieu où les données personnelles sont hébergées.
Indiquez quels pays les données personnelles sont éventuellement transférées.

### *JUSQU'À QUAND ?*

Indiquez, pour chaque catégorie de données personnelles, combien de temps vous les conservez.

### *COMMENT ?*

Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données personnelles et donc d'impact sur la vie privée des personnes concernées ?
Les outils pour vous aider : Modèle de fiche de cartographie modèle de l'INPDP (CF annexe 4)

## B. Le registre de traitements

Le registre de traitements permet de recenser vos traitements de données et de disposer d'une vue d'ensemble de ce que vous faites avec les données personnelles.

Le registre de traitements participe à la documentation de la conformité, c'est un document de recensement et d'analyse, il doit refléter la réalité de vos traitements de données personnelles et vous permet d'identifier précisément :

- Les parties prenantes (responsable de traitement, sous-traitants, co-responsables de traitement) qui interviennent dans le traitement des données,
  Les catégories de données traitées,

- À quoi servent ces données (ce que vous en faites),
- Qui accède aux données
- À qui elles sont communiquées,
- Combien de temps vous les conservez,
- Comment elles sont sécurisées.

De même, le registre est un outil de pilotage et de démonstration de votre conformité à la législation et la règlementation en vigueur en matière de protection des données personnelles. Il vous permet de documenter vos traitements de données et de vous poser les bonnes questions : ai-je vraiment besoin de cette donnée dans le cadre de mon traitement ? Est-il pertinent de conserver toutes les données aussi longtemps ? Les données sont-elles suffisamment protégées ?

Sa création et sa mise à jour sont ainsi l'occasion d'identifier et de hiérarchiser les risques au regard de la législation et la règlementation en vigueur en matière de protection des données personnelles. Cette étape essentielle vous permettra d'en déduire un plan d'action de mise en conformité de vos traitements aux règles de protection des données.

Ce guide présente ici les éléments essentiels relatifs au registre et propose également un modèle de base proposé par l'INPDP, répondant aux conditions posées par la législation et la règlementation en vigueur en matière de protection des données personnelles.

### *Que contient le registre ?*

Le registre du responsable de traitement doit recenser l'ensemble des traitements mis en œuvre par l'entreprise d'assurances.

En pratique, une fiche de cartographie modèle de l'INPDP (cf. annexe 4) doit donc être établie pour chaque traitement de données ayant une finalité distinctive, afin d'élaborer le registre de traitements modèle de base de l'INPDP (cf. annexe 5)

### *Quelle forme doit prendre le registre ?*

Selon les recommandations de l'INPDP, le registre se présente sous une forme écrite. Le format du registre est libre et peut être constitué au format papier ou électronique.

Il est recommandé dans la mesure du possible, d'enrichir le registre de mentions complémentaires afin d'en faire un outil plus global de pilotage de la conformité.

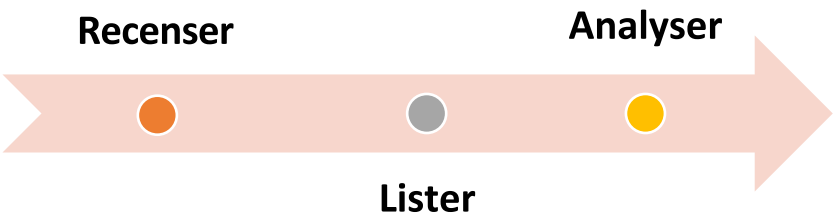
### *Qui doit tenir le registre ?*

Le registre doit être tenu par les responsables de traitement ou les sous-traitants eux-mêmes. Ils peuvent ainsi disposer d'une vue d'ensemble de tous les traitements de données à caractère personnel qu'ils effectuent.

Une personne au sein de l'organisme peut être spécifiquement chargée de la tenue du registre. Dans le cas où l'organisme a désigné un délégué à la protection des données (DPO), interne ou externe, celui-ci peut être chargé de la tenue du registre. Le registre pourra ainsi constituer l'un des outils permettant au délégué à la protection des données (DPO) d'exercer ses missions de contrôle du respect de la législation et de la réglementation en vigueur en matière de protection des données

personnelles ainsi que d'information et de conseil du responsable du traitement ou du sous-traitant.

*Comment constituer un registre ?*




**RASSEMBLER LES INFORMATIONS DISPONIBLES**
Rencontrer les responsables opérationnels des différents services afin d'identifier et de recenser les données personnelles traitées.

Si l'entreprise d'assurances dispose d'un site internet, identifier et recenser les données collectées dans les formulaires en ligne (questionnaire, formulaire de contact, création d'un compte...), les mentions d'information «protection des données», l'utilisation de cookies…

**ELABORER LA LISTE DES TRAITEMENTS**
Lister dans un tableau de suivi les différents traitements de données personnelles de l'entreprise d'assurances. Les traitements de données doivent être identifiés par finalité et non par logiciel utilisé, car un même logiciel peut être utilisé pour différents traitements et inversement.

Sur la base des informations collectées lors des entretiens, remplir une fiche de cartographie par chaque traitement de données ayant une finalité distinctive.

**AFFINER / PRÉCISER**
Sur la base de ce registre, identifier et analyser les risques qui peuvent peser sur les traitements de données mis en œuvre et élaborer un plan d'action de mise en conformité à la législation et à la réglementation en vigueur en matière de protection des données personnelles.

*A qui communiquer le registre ?*
Par nature, le registre est un document interne et évolutif, qui doit avant tout aider l'entreprise d'assurances à piloter sa conformité.

Le registre doit toutefois pouvoir être communiqué à l'INPDP lorsqu'elle le demande. Elle pourra en particulier l'utiliser dans le cadre de sa mission de contrôle des traitements de données.

## 2. L'Information des personnes concernées

Dès le stade de la collecte des données personnelles, les personnes concernées doivent être informées de l'existence du traitement, de ses caractéristiques et des droits dont elles disposent en vertu de la législation et la réglementation en vigueur applicable en matière de protection des données à caractère personnel **(cf. Modèle de mention d'informations annexe 2)**

## A. Quelles informations dois-je donner ?

- Nature des données à caractère personnel concerné par le traitement
- Les finalités du traitement des données à caractère personnel : c'est à l'entreprise d'expliquer d'une manière simple et explicite dans quel but elle collecte les données de la personne.
- Le caractère obligatoire ou facultatif de la réponse des personnes concernées
- Conséquence du défaut de réponse de la personne concernée
- Le nom de la personne physique ou morale bénéficiaire des données ou de celui qui dispose du droit d'accès et son domicile
- Le nom et prénom du responsable du traitement ou sa dénomination sociale et, le cas échéant, son représentant et son domicile.
- Les droits des personnes : Tels que définis dans le chapitre 5 du présent guide.
- Les durées de conservations
- Les destinataires ou catégories de destinataires : section 7 du ce chapitre: Mesures supplémentaires en cas de transfert et communication des données
- L'existence d'un transfert hors la Tunisie[21]

## B. Sous quel format ?

La notification s'effectue par n'importe quel moyen laissant une trace écrite.

## C. Comment délivrer l'information ?

Ces informations doivent être fournies dans la mesure du possible de façon :

- Succincte
- Adapté au public visé
- Clairement distincte des autres mentions d'informations du contrat
- Concrète et explicite dans un langage simple et non technique
- Facilement accessible.

## D. Quand délivrer l'information ?

Lorsque le responsable de traitement collecte les données auprès de la personne concernée il doit lui fournir les informations mentionnées ci-dessus.
En pratique, le responsable de traitement doit identifier toutes les sources de collecte des données au sein de son entreprise, les classer et s'assurer qu'une mention d'information est présente pour chaque source de collecte. Si la collecte des données personnelles est faite en ligne[22] , la mention d'information doit être présente sur le formulaire de collecte des données présent sur le site internet. Si la collecte est faite directement sur les lieux, la mention doit être présente sur le formulaire papier.

[21] Conformément à la liste des pays adéquats diffusée sur le site de l'INPDP
[22] Le site internet de l'entreprise d'assurances doit comporter des conditions générales d'utilisation (annexe 8)
En cas de souscription de contrat d'assurances en ligne, il faut prévoir des conditions générales de vente selon la loi n°83-2000 du 09/08/2000 relative aux échanges et au commerce électronique

### E. Ce qu'il faut faire dans le cas d'utilisation des cookies dans le site

**Définition**
Un cookie est un petit fichier stocké par un serveur dans le terminal (ordinateur, téléphone, etc.) d'un utilisateur et associé à un domaine web (c'est à dire dans la majorité des cas à l'ensemble des pages d'un même site web). Ce fichier est automatiquement renvoyé lors de contacts ultérieurs avec le même domaine.
Les cookies ont de multiples usages : ils peuvent servir à mémoriser votre identifiant client auprès d'un site marchand, le contenu courant de votre panier d'achat, la langue d'affichage de la page web, un identifiant permettant de tracer votre navigation à des fins statistiques ou publicitaires, etc. Certains de ces usages sont strictement nécessaires aux fonctionnalités expressément demandées par l'utilisateur ou bien à l'établissement de la communication et donc exemptés de consentement. D'autres, qui ne correspondent pas à ces critères, nécessitent un consentement de l'utilisateur avant lecture ou écriture.
**Dans le cas d'utilisation des cookies dans le site du responsable du traitement il faut :**

- Informer les internautes de l'existence des cookies
- Préparer une politique de cookies et la mettre dans un lien consultable
- Ajouter des boutons à cliquer pour choisir soit d'accepter et fermer soit de personnaliser les cookies ou refuser

## 3. Le consentement de la personne concernée

### A. Les conditions de consentement[23]

Le consentement doit être éclairé, explicite, réversible, volontaire et non conditionné
*éclairé: il est donné sur la base d'une connaissance de l'opération de traitement c'est-à-dire l'obligation d'information(l'article31)
*explicite: il est donné de manière explicite laissant une trace écrite, il ne peut pas être pré sumé (l'article 2)

*claire et ne prête à aucune confusion: le consentement au traitement des données à caractère personnel sous une forme déterminée ou pour une finalité déterminée ne s'applique pas aux autres formes ou finalités (l'article 30)

*réversible :la personne concernée peut revenir dessus(l'article27). **La personne concernée a le droit de retirer son consentement à tout moment** (l'article 31). Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement qu'il est aussi simple de retirer que de donner son consentement **(cf. Modèle de formulaire d'exercice des droits à la protection des données personnelles annexe 3)**

*volontaire : la personne concernée ne peut être obligée à le donner.
Le responsable du traitement a l'obligation légale d'informer la personne concernée sur le caractère obligatoire ou optionnel de renseigner les données (l'article 31).

[23] Suivant la loi organique n°2004-63 du 27 juillet 2004 portant sur la protection des données à caractère personnel

*non conditionné : le responsable du traitement ne peut pas conditionner une prestation à l'obtention du consentement à fournir ces données personnelles (l'article 17)

### B. Les cas où le consentement n'est pas obligatoire pour le traitement des données personnelles[24]

La collecte et le traitement des données à caractère personnel ne sont pas soumis au consentement de la personne concernée dans les cas suivants :

* Pour l'exécution d'un contrat d'assurance ou d'une convention avec les sous-traitants dans lesquels la personne concernée est partie,
* Prévus par la loi
* Effectués dans l'intérêt de la personne concernée
* Le contact de la personne concernée se révèle impossible
* L'obtention du consentement de la personne concernée implique des efforts disproportionnés

## 4.Gestion des risques liés aux données personnelles

### A. Elaborer un processus de sécurisation

Il existe plusieurs méthodes pour maîtriser la sécurité. Elles se composent généralement de trois grandes catégories de processus :

#### *a. Une gestion des risques :*

Identification des principaux risques, à discerner ceux qui doivent être traités et ceux qui sont acceptables. Mettre en œuvre les moyens de sécurité traitant les risques encourus par les données à caractère personnel selon une échelle de priorité. Les processus de gestion des risques forment un cycle qui est à répéter selon les particularités des systèmes et des risques identifiés. La gestion des risques débouche sur des processus de définition ou de mise à jour de la politique de sécurité et, souvent, sur des adaptations de l'organisation et des procédures de manière à mieux prendre en compte les nouveaux risques et les mesures de sécurité mises en œuvre ;

#### *b. La gestion quotidienne de la sécurité*

Comprenant notamment des activités comme l'administration des dispositifs de sécurité, la gestion des autorisations, l'analyse des incidents détectés ;

#### *c. Le système de management visant à une amélioration continue de la sécurité*

Il existe plusieurs modèles de système de management de la sécurité de l'information (ISMS - Information Security Management System). Le plus connu est basé sur une structure PDCA (Plan – Do – Check - Act). Cette amélioration continue se justifie par la nécessité d'adaptation à de multiples facteurs d'évolution comme les modifications de l'organisme et des risques associés, les modifications dans les systèmes d'information, les nouveautés technologiques tant pour les systèmes opérationnels que pour les dispositifs de sécurité.

[24] Suivant l'article 29 de la loi organique n°2004-63

## B. Analyse d'impact[25]

L'analyse d'impact relative à la protection des données est un processus qui permet d'identifier, d'évaluer et de réduire les risques liés à la protection des données.

L'objectif principal d'une APD est d'analyser le traitement des données à caractère personnel et de déterminer le niveau de risque. Les résultats d'une AIPD permettront à l'organisme de concevoir ses systèmes avec des niveaux de protection des données appropriés. Pour l'essentiel, une AIPD peut être considérée comme un outil fondé sur le risque pour mesurer et examiner le niveau de protection des données et, le cas échéant, proposer différents changements de conception.

L'AIPD a pour but d'aider à établir et à démontrer la conformité au RGPD.

Voici quelques-unes des principales étapes d'une analyse d'impact relative à la protection des données. Toutefois, le processus d'AIPD peut être adapté au contexte spécifique des activités de traitement de l'organisme.

1 - Identifier la nécessité d'une AIPD
2 - Décrire le flux d'information
3 - Identifier la protection des données et les autres risques connexes
4 - Identifier et évaluer les solutions en données matière de protection des données
5 - Signer et enregistrer les résultats de l'AIPD

**Rôle du DPO dans l'AIPD**

Le délégué à la protection des données devrait donner des conseils au responsable du traitement ou au sous-traitant sur les éléments suivants :

- S'il convient ou non de procéder à une AIPD
- La méthodologie qui devrait être suivie dans le cas où une AIPD doit être menée
- Si l'AIPD devrait être réalisée en interne ou en externe
- Si les conclusions de l'AIPD sont conformes aux exigences du RGPD
- Les garanties nécessaires pour atténuer le risque pour les droits et les intérêts des personnes concernées
- Les activités qui impliquent des audits de protection des données et celles qui devraient faire l'objet d'une attention particulière de la part de la direction en ce qui concerne les mesures de sécurité renforcées, la formation régulière du personnel et l'affectation des ressources.

Il est à noter que le DPO ne procède pas à l'AIPD ; elle est réalisée par le responsable du traitement (organisme)

[25] Il est à préciser que l'analyse d'impact n'est pas exigée actuellement par notre législation et règlementation en vigueur

# 5. La sécurité des données personnelles

## A. Sensibiliser les utilisateurs

- Sensibiliser les utilisateurs travaillant avec des données à caractère personnel aux risques liés aux libertés et à la vie privée, les informer des mesures prises pour traiter les risques et des conséquences potentielles en cas de manquement.

- Organiser une séance de sensibilisation, envoyer régulièrement les mises à jour des procédures pertinentes pour les fonctions des personnes, faire des rappels par messagerie électronique, etc.

- Documenter les procédures d'exploitation, les tenir à jour et les rendre disponibles à tous les utilisateurs concernés. Concrètement, toute action sur un traitement de données à caractère personnel, qu'il s'agisse d'opérations d'administration ou de la simple utilisation d'une application, doit être expliquée dans un langage clair et adapté à chaque catégorie d'utilisateurs, dans des documents auxquels ces derniers peuvent se référer.

- Rédiger une charte informatique et lui donner une force contraignante (ex. annexion au règlement intérieur).

## B. Authentifier les utilisateurs

- Pour assurer qu'un utilisateur accède uniquement aux données dont il a besoin, il doit être doté d'un identifiant qui lui est propre et doit s'authentifier avant toute utilisation des moyens informatiques.

- Définir un identifiant unique par utilisateur et interdire les comptes partagés entre plusieurs utilisateurs.

- Respecter la recommandation des normes ISO dans le cas d'une authentification des utilisateurs basée sur des mots de passe.

## C. Gérer les habilitations

- Définir des profils d'habilitation afin de limiter l'accès des utilisateurs aux seules données strictement nécessaires à l'accomplissement de leurs missions.

- Supprimer les permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder à un local ou à une ressource informatique, ainsi qu'à la fin de leur contrat.

- Réaliser une revue annuelle des habilitations (politique de contrôle d'accès) afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.

## D. Tracer les accès et gérer les incidents

- Prévoir un système de journalisation des activités des utilisateurs, des anomalies et des événements liés à la sécurité

- Informer les utilisateurs de la mise en place d'un tel système.

- Protéger les équipements de journalisation et les informations journalisées

- Établir des procédures détaillant la surveillance de l'utilisation du traitement et examiner périodiquement les journaux d'événements pour y détecter d'éventuelles anomalies.

- Assurer que les gestionnaires du dispositif de gestion des traces notifient, dans les plus brefs délais, toute anomalie ou tout incident de sécurité au responsable de traitement (Prévoir une procédure de violation des données).

- Diffuser à tous les utilisateurs la conduite à tenir et la liste des personnes à contacter en cas d'incident de sécurité ou de survenance d'un événement inhabituel touchant aux systèmes d'information et de communication de l'organisme

## F. Sécuriser les postes de travail

- Prévoir un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné.

- Installer un «pare-feu» («firewall») logiciel, et limiter l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail.

- Utiliser des antivirus régulièrement mis à jour

- Configurer les logiciels pour que les mises à jour de sécurité se fassent automatiquement dès que cela est possible.

- Favoriser le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé accessible via le réseau de l'organisme plutôt que sur les postes de travail. Dans le cas où des données sont stockées localement, fournir des moyens de synchronisation ou de sauvegarde aux utilisateurs et les former à leur utilisation.

- Limiter la connexion de supports mobiles (clés USB, disques durs externes, etc.) à l'indispensable.
- Désactiver l'exécution automatique (« autorun ») depuis des supports amovibles.

Pour l'assistance sur les postes de travail :

• Les outils d'administration à distance doivent recueillir l'accord de l'utilisateur avant toute intervention sur son poste, par exemple en répondant à un message s'affichant à l'écran ;

• L'utilisateur doit également pouvoir constater si la prise de main à distance est en cours et quand elle se termine, par exemple grâce à l'affichage d'un message à l'écran.

## G. Sécuriser l'informatique mobile

- Sensibiliser les utilisateurs aux risques spécifiques liés à l'utilisation d'outils informatiques

mobiles (ex : vol de matériel) et aux procédures prévues pour les limiter.

- Mettre en œuvre des mécanismes maîtrisés de sauvegardes ou de synchronisation des postes nomades, pour se prémunir contre la disparition des données stockées.

- Prévoir des moyens de chiffrement des postes nomades et supports de stockage mobiles (ordinateur portable, clés USB, disque dur externes, CD-R, DVD-RW, etc.), par exemple :
  - Le chiffrement du disque dur dans sa totalité lorsque le système d'exploitation le propose ;
  - Le chiffrement fichier par fichier ;

- Concernant les smartphones, en plus du code PIN de la carte SIM, activer le verrouillage automatique du terminal et exiger un secret pour le déverrouiller (mot de passe, schéma, etc.

## H. Protéger le réseau informatique interne

- Limiter les accès Internet en bloquant les services non nécessaires (VoIP, pair à pair, etc.)

- Gérer les réseaux Wi-Fi. Ils doivent utiliser un chiffrement à l'état de l'art (WPA2 ou WPA2-PSK avec un mot de passe complexe) et les réseaux ouverts aux invités doivent être séparés du réseau interne.

- Imposer un VPN pour l'accès à distance ainsi que, si possible, une authentification forte de l'utilisateur (carte à puce, boitier générateur de mots de passe à usage unique (OTP), etc.).

- S'assurer qu'aucune interface d'administration n'est accessible directement depuis Internet. La télémaintenance doit s'effectuer à travers un VPN.

- Limiter les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.). Par exemple, si un serveur web utilise obligatoirement HTTPS, il faut autoriser uniquement les flux entrants sur cette machine sur le port 443 et bloquer tous les autres ports.

## I. Sécuriser les serveurs

- La sécurité des serveurs doit être une priorité car ils centralisent un grand nombre de données.

- Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées. Utiliser des comptes de moindres privilèges pour les opérations courantes.

- Adopter une politique spécifique de mots de passe pour les administrateurs. Changer les mots de passe, au moins, lors de chaque départ d'un administrateur et en cas de suspicion de compromission.
- Installer les mises à jour critiques sans délai que ce soit pour les systèmes d'exploitation ou pour les applications, en programmant une vérification automatique hebdomadaire.

En matière d'administration de bases de données :
- Utiliser des comptes nominatifs pour l'accès aux bases de données et créer des comptes

spécifiques à chaque application ;

- Mettre en œuvre des mesures contre les attaques par injection de code SQL, de scripts, etc.

- Effectuer des sauvegardes et les vérifier régulièrement.

- Mettre en œuvre le protocole TLS (en remplacement de SSL13), ou un protocole assurant le chiffrement et l'authentification, au minimum pour tout échange de données sur internet et vérifier sa bonne mise en œuvre par des outils appropriés14.

## J. Sécuriser les sites web

- Mettre en œuvre le protocole TLS (en remplacement de SSL23) sur tous les sites web, en utilisant uniquement les versions les plus récentes et en vérifiant sa bonne mise en œuvre.

- Rendre l'utilisation de TLS obligatoire pour toutes les pages d'authentification, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques.

- Limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées. Si l'accès à un serveur web passe uniquement par HTTPS, il faut autoriser uniquement les flux réseau IP entrants sur cette machine sur le port 443 et bloquer tous les autres ports.

- Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées. En particulier, limiter l'utilisation des comptes administrateurs aux équipes en charge de l'informatique et ce, uniquement pour les actions d'administration qui le nécessitent.

- Si des cookies non nécessaires au service sont utilisés, recueillir le consentement de l'internaute après information de celui-ci et avant le dépôt du cookie.

- Limiter le nombre de composants mis en œuvre, en effectuer une veille et les mettre à jour.

## K. Archiver de manière sécurisée

- Définir un processus de gestion des archives (numérique et papier) : quelles données doivent être archivées, comment et où sont-elles stockées, comment sont gérées les données descriptives?

- Mettre en œuvre des modalités d'accès spécifiques aux données archivées du fait que l'utilisation d'une archive doit intervenir de manière ponctuelle et exceptionnelle.

- S'agissant de la destruction des archives, choisir un mode opératoire garantissant que l'intégralité d'une archive a été détruite.

## L. Encadrer la maintenance et la destruction des données

- Enregistrer les interventions de maintenance.

- Insérer une clause de sécurité dans les contrats de maintenance effectuée par des prestataires.

- Encadrer par un responsable de l'organisme les interventions par des tiers.
- Rédiger et mettre en œuvre une procédure de destruction sécurisée des données.

- Supprimer de façon sécurisée les données des matériels avant leur mise au rebut, leur envoi en réparation chez un tiers ou en fin du contrat de location.

## M. Gérer la sous-traitance

- Faire appel uniquement à des sous-traitants présentant des garanties suffisantes (notamment en termes de connaissances spécialisées, de fiabilité et de ressources). Exiger la communication par le prestataire de sa politique de sécurité des systèmes d'information.

- Prendre et documenter les moyens (audits de sécurité, visite des installations, etc.) permettant d'assurer l'effectivité des garanties offertes par le sous-traitant en matière de protection des données. Ces garanties incluent notamment :

• Le chiffrement des données selon leur sensibilité ou à défaut l'existence de procédures garantissant que la société de prestation n'a pas accès aux données qui lui sont confiées si cela n'est pas nécessaire à l'exécution de son contrat ;
• Le chiffrement des transmissions de données (ex : connexion de type HTTPS, VPN, etc.) ;
• Des garanties en matière de protection du réseau, de traçabilité (journaux, audits), de gestion des habilitations, d'authentification, etc.

- Prévoir un contrat avec les sous-traitants, qui définit notamment l'objet, la durée, la finalité du traitement et les obligations des parties. S'assurer qu'il contient en particulier des dispositions fixant :

• Leur obligation en matière de confidentialité des données personnelles confiées ;
• Des contraintes minimales en matière d'authentification des utilisateurs ;
• Les conditions de restitution et/ou de destruction des données en fin du contrat ;
• Les règles de gestion et de notification des incidents, celles-ci devraient comprendre une information du responsable de traitement en cas de découverte de faille de sécurité ou d'incident de sécurité et cela dans les plus brefs délais lorsqu'il s'agit d'une violation de données à caractère personnel.

## N. Sécuriser les échanges avec d'autres organismes

- Chiffrer les données avant leur enregistrement sur un support physique à transmettre à un tiers (DVD, clé USB, disque dur portable).

- Lors d'un envoi via un réseau :
• Chiffrer les pièces sensibles à transmettre, si cette transmission utilise la messagerie électronique. À ce sujet, il convient de se référer aux préconisations de la fiche n°17 (Utiliser des fonctions cryptographiques) du guide de la sécurité des donnés personnelles diffusé par la CNIL;
• Utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers, par exemple SFTP ou HTTPS, en utilisant les versions les plus récentes des protocoles;
- Assurer la confidentialité des secrets (clé de chiffrement, mot de passe, etc.) en les transmettant via un canal distinct (par exemple, envoi du fichier chiffré par e-mail et communication du

mot de passe par téléphone ou SMS).

- Si vous êtes amené à utiliser le fax, mettre en place les mesures suivantes :
• Installer le fax dans un local physiquement contrôlé et uniquement accessible au personnel habilité ;
• Faire afficher l'identité du fax destinataire lors de l'émission des messages ;
• Doubler l'envoi par fax d'un envoi des documents originaux au destinataire ;
• Préenregistrer dans le carnet d'adresse des fax (si la fonction existe) les destinataires potentiels.

## O. Protéger les locaux

- Installer des alarmes anti-intrusion et les vérifier périodiquement.
- Mettre en place des détecteurs de fumée ainsi que des moyens de lutte contre les incendies, et les inspecter annuellement.
- Protéger les clés permettant l'accès aux locaux et les codes d'alarme.
- Distinguer les zones des bâtiments selon les risques (par exemple prévoir un contrôle d'accès dédié pour la salle informatique).
- Tenir à jour une liste des personnes ou catégories de personnes autorisées à pénétrer dans chaque zone.
- Établir les règles et moyens de contrôle d'accès des visiteurs, au minimum en faisant accompagner les visiteurs, en dehors des zones d'accueil du public38 par une personne appartenant à l'organisme.
- Protéger physiquement les matériels informatiques par des moyens spécifiques (système anti-incendie dédié, surélévation contre d'éventuelles inondations, redondance d'alimentation électrique et/ou de climatisation, etc.).

## P. Encadrer le développement informatique

- Intégrer la protection de la vie privée, y compris ses exigences de sécurité des données, dès la conception de l'application ou du service. (Privacy by design)
- Pour tout développement à destination du grand public, mener une réflexion sur les paramètres relatifs à la vie privée, et notamment sur le paramétrage par défaut.
- Éviter le recours à des zones de texte libre ou de commentaires.
- Effectuer les développements informatiques et les tests dans un environnement informatique distinct de celui de la production (par exemple, sur des ordinateurs ou des machines virtuelles différents) et sur des données fictives ou anonymisées.
- Ne pas Utiliser des données à caractère personnel réelles pour les phases de développement et de test. Des jeux fictifs doivent être utilisés autant que possible.
- Éviter de développer une application puis réfléchir dans un second temps aux mesures de sécurité à mettre en place.

## Q. Chiffrer, garantir l'intégrité ou signer

Les fonctions de hachage permettent d'assurer l'intégrité des données.
Les signatures numériques, en plus d'assurer l'intégrité, permettent de vérifier l'origine de l'information et son authenticité.
Enfin, le chiffrement, parfois improprement appelé cryptage, permet de garantir la confidentialité d'un message.

## R. Conserver les données personnelles

### *a. Les types des données à caractère personnel conservées*

Le cycle de vie des données à caractère personnel peut se décomposer en trois phases successives :

• Les bases actives ou données courantes : il s'agit des données d'utilisation courante par les services en charge de la mise en œuvre du traitement ;

• Les données intermédiaires : il s'agit des données qui ne sont plus utilisées mais qui présentent encore un intérêt administratif pour l'organisme. Les données sont conservées sur support distinct et sont consultées de manière ponctuelle et motivée ;

• Les données définitives : il s'agit des données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction.

### *b. La durée de conservation des données à caractère personnel*

Les données à caractère personnel doivent être détruites dès l'expiration du délai fixé à sa conservation dans la déclaration ou l'autorisation de l'INPDP ou les lois spécifiques ou en cas de réalisation des finalités pour lesquelles elles ont été collectées ou lorsqu'elles deviennent inutiles pour l'activité du responsable du traitement[26]

### *c. La destruction des données caractère personnel*

C'est un acte courant de la vie d'une compagnie d'assurances permettant notamment de gagner de la place dans ses locaux.
L'entreprise d'assurance doit mettre en place un référentiel qui indique le calendrier, les modalités et la périodicité de la destruction des documents tout en tenant compte des dispositions légales de conservation et des besoins métiers de l'entreprise.

# 6. La sauvegarde des données et la continuité d'activité

La sauvegarde des données :

• Effectuer des sauvegardes fréquentes des données, que celles-ci soient sous forme papier ou électronique. Il peut être opportun de prévoir des sauvegardes incrémentales quotidiennes et des sauvegardes complètes à intervalles réguliers.

• Stocker les sauvegardes sur un site extérieur, si possible dans des coffres ignifugés et étanches.

• Protéger les données sauvegardées au même niveau de sécurité que celles stockées sur les serveurs d'exploitation (par exemple en chiffrant les sauvegardes, en prévoyant un stockage dans un lieu sécurisé, en encadrant contractuellement une prestation d'externalisation des sauvegardes).

[26] Article 45 de la loi organique de protection des données personnelles

• Lorsque les sauvegardes sont transmises par le réseau, il convient de chiffrer le canal de transmission si celui-ci n'est pas interne à l'organisme.

• La reprise et la continuité d'activité

• Rédiger un plan de reprise et de continuité d'activité informatique même sommaire, incluant la liste des intervenants.

• S'assurer que les utilisateurs, prestataires et sous-traitants savent qui alerter en cas d'incident.

• Tester régulièrement la restauration des sauvegardes et l'application du plan de continuité ou de reprise de l'activité.

• À propos des matériels :
• Utiliser un onduleur pour protéger le matériel servant aux traitements essentiels
• Prévoir une redondance matérielle des matériels de stockage, par exemple au moyen d'une technologie RAID.

## 7. L'audit de la sécurité du système d'information

L'entreprise d'assurance doit mettre en place un audit de sécurité informatique qui permet d'évaluer le niveau de sécurité de son système d'information et ce, conformément à la procédure, aux critères techniques et à la fréquence prévus par la législation en vigueur.

L'évaluation de la sécurité des systèmes d'information porte essentiellement sur :

• L'état des lieux du système d'information qui permet d'examiner la totalité des domaines à risques potentiels.

• Le test de résistance du site internet qui permet d'identifier les faiblesses et/ou trouver les points critiques.
• L'audit de sécurité WIFI qui permet de tester la résistance aux vulnérabilités et mettre en avant les faiblesses exploitables par l'attaquant.

En application de l'article 25 du décret-loi n°17-2023 du 11 mars 2023 relatif à la cybersécurité, plusieurs sanctions sont prévues en cas d'infraction ; sont punis d'une amende de cinquante mille (50 000) dinars à cent mille (100 000) dinars les organismes mentionnés à l'article 6 de ce décret-loi, et classés au troisième niveau, et ce dans les cas suivants :

• La non-réalisation de l'audit obligatoire et périodique de sécurité des systèmes d'information.
• La non-exécution des recommandations du rapport d'audit ou leur exécution partielle dans un délai n'excédant pas une année.
• Le non-respect des mesures d'urgence prescrites par le point de contact national pour la réponse aux urgences cybernétiques ou les centres de réponse aux urgences cybernétiques

suite à la survenance d'un incident ou d'une attaque cybernétique.
• Le non-relève des défaillances dans le délai mentionné à l'article 17 du cet décret-loi.
• La non-création d'un centre de réponse aux urgences cybernétique ou la non-adhésion aux centres de réponse aux urgences cybernétiques.

## 8. La mise à jour et la fiabilisation des données

### A. La mise à jour des données

Les données personnelles servent de base à la prise de décision concernant les personnes concernées.

• Le responsable du traitement est tenu de mettre à jour continuellement ces données et les effacer si elles s'avèrent illégales ou inexactes.
• Le responsable du traitement et le sous-traitant doivent corriger, compléter, modifier ou mettre à jour les fichiers dont ils disposent, et effacer les données à caractère personnel de ces fichiers s'ils ont eu connaissance de l'inexactitude ou de l'insuffisance de ces données[27]
• Le responsable qui intentionnellement traite des données non mises à jour est sanctionné
• C'est une obligation importante au vu de l'impact de ces données sur les traitements automatiques qui entrainent la prise de décision faisant grief à travers des traitements informatiques

### B. La fiabilisation des données

#### *a. Qu'est-ce que la fiabilisation des données ?*

Les entreprises d'assurances sont de plus en plus orientées data. Dans ce contexte, la donnée devient une ressource précieuse et stratégique à exploiter. C'est là qu'intervient la fiabilisation des données, visant à améliorer la qualité des data de l'entreprise. Autrement dit, elle consiste à garantir que les informations contenues dans ses bases de données soient correctes, complètes, exactes et facilement exploitables (bon format, pas de doublons).
Mais la mise en place d'un travail de fiabilisation de la donnée peut aller plus loin, et assurer aussi :

• L'intégrité des données (veiller à ce qu'elles ne soient pas modifiées),
• Leur conformité réglementaire,
• Leur sécurité au sein des différents systèmes d'information
• Leur consolidation, c'est-à-dire le fait de les regrouper et de les organiser intelligemment entre elles pour en faciliter l'utilisation.

Enfin, la fiabilisation des données intègre aussi des processus d'actualisation : les informations évoluent constamment, mieux vaut privilégier les plus récentes.

#### *b. Qu'est-ce que le processus de fiabilisation des données ?*

Le processus de fiabilisation des données désigne le mécanisme de contrôle et d'amélioration permanente de la qualité des données d'un système d'informations.
Les données disponibles dans l'entreprise d'assurance seront leur base de travail, il est ainsi essentiel de les protéger. Il est alors primordial de limiter l'accès à la donnée pour la sécuriser au sein des différents systèmes d'information : gestion des accès, charte ou/et politique (cf. section 4 sécurité des DP).
Mise en rapport avec la sécurité des données, la traçabilité de ces dernières est une notion à prendre en compte lorsqu'il s'agit d'utilisation des données. Un utilisateur doit être en mesure de garantir leur provenance, car le cas échéant, les risques de se retrouver avec des données inutilisables augmentent.

[27] Art. 21 de la loi organique 63/2004

## 9. Les exigences vis-à-vis de l'INPDP

**Le traitement des données personnelles combine la déclaration et la demande d'autorisation.**
Le formulaire de déclaration de l'INPDP est un passage obligatoire pour toutes les procédures, c'est le régime général de tout traitement qui a pour objectif la transparence, il permet de renseigner à l'INPDP tous les éléments nécessaires pour statuer sur la conformité de l'opération de traitement à la législation et la réglementation en vigueur en matière de protection des données à caractère personnel.
Le formulaire de demande d'autorisation est le régime spécial.
Les formulaires cités ci-dessous sont disponible sur le site de l'INPDP[28] :

- La déclaration de traitement de données
- La demande d'autorisation préalable de traitement de données biométriques
- La demande d'autorisation préalable d'installation d'un système de vidéosurveillance
- La demande d'autorisation préalable au traitement de données de santé
- La demande d'autorisation préalable de traitement de convictions et appartenances
- La demande d'autorisation préalable de transfert de données vers l'étranger
- La demande d'autorisation préalable de traitement de données de communication
- La demande d'autorisation préalable de traitement de données de géo- localisation

Ces formulaires permettent de traiter les données personnelles classiques et sensibles.

Tout formulaire mal rempli ou ne renseignant pas soigneusement les rubriques qui le composent entraînera un report du dossier à la réunion du conseil suivant et par la suite son rejet si le responsable de traitement ne le complète pas.

Les formulaires sont des déclarations sur l'honneur qui nécessitent le représentant légal du responsable de traitement et son tampon. Toute fausse déclaration entrainera des sanctions pénales prévues par le code pénal.

Les formulaires peuvent être déposés au bureau d'ordre de l'INPDP contre décharge ou être faxés à l'Instance ou envoyés par la poste ou encore scannés et envoyés par mails aux coordonnées disponibles sur la page contact de l'INPDP[29].

Pour prouver que le traitement des données est légal, l'entreprise d'assurance doit tenir un registre des traitements dont lequel sont précisés entre autres les données personnelles stockées, leurs finalités et les traitements réalisés. (c.f annexe 5)

Le formulaire de déclaration ou d'autorisation doit être accompagné par tous les justificatifs nécessaires.
En cas de contrôle de l'INPDP, ce registre des traitements sera demandé.

[28] www.inpdp.tn
[29] www.inpdp.tn

## 10. Les mesures supplémentaires en cas de communication des données sur le territoire tunisien et en cas de transfert à l'étranger

**Communication des données personnelles :**
L'entreprise d'assurance peut communiquer des données à caractère personnel à des tiers sur le territoire Tunisien et ce dans le cadre de l'exécution du contrat d'assurance auquel la personne concernée est partie.

**Transfert des données personnelles vers l'étranger**
Il s'agit de communiquer les données à caractère personnel vers l'étranger ainsi que permettre la consultation à distance par une personne non-résidente sur le territoire Tunisien et ce dans le cadre de l'exécution d'un contrat

**Les mesures supplémentaires**
Dans ces deux cas, le bénéficiaire des données à caractère personnel s'engage à mettre en œuvre toutes les garanties nécessaires à la protection des données et des droits qui s'y rattachent conformément à la législation et la règlementation en vigueur et aux directives de l'Instance, et s'engage à s'assurer que ces données ne seront pas utilisées à des fins autres que celles pour lesquelles elles ont été communiquées.

Le transfert à l'étranger nécessite une autorisation préalable auprès de l'INPDP.

## 11. Les bénéficiaires des données à caractère personnel

Le Bénéficiaire est toute personne physique ou morale recevant des données à caractère personnel. Il peut s'agir selon les cas du responsable de traitement, du sous-traitant, du tiers.

### A. Les bénéficiaires communs à tous les traitements

Peuvent avoir accès aux données à caractère personnel dans les limites de leurs attributions respectives en fonction des traitements concernés :

***a. Dans le cadre des missions habituelles :***

- les personnes chargées de la gestion commerciale des clients/des prospects ou de la gestion et l'exécution des contrats ;
- Les intermédiaires d'assurance,
- Les prestataires de services ;
- Les entités du groupe auquel appartient le responsable de traitement dans le cadre de l'exercice de leurs missions ;
- les sous-traitants chargés de la gestion et/ou de l'exécution des contrats d'assurance santé tels qu'un réseau de soins ou un prestataire d'assurance santé ;
- s'il y a lieu les co-assureurs et réassureurs, les intermédiaires de réassurance ainsi que les organismes professionnels et les fonds de garanties ;

• les auxiliaires intervenants au contrat d'assurance tels que les avocats, les experts, les huissiers de justice, les notaires, les médecins … ;
• les services chargés du contrôle (services chargés des procédures internes du contrôle, commissaire aux comptes...).

### *b. Les Personnes intéressées au contrat :*

• les souscripteurs, les assurés, les adhérents et les bénéficiaires des contrats d'assurances ; et s'il y a lieu leurs ayants droit et représentants ;
• s'il y a lieu les bénéficiaires d'une cession ou d'une subrogation des droits relatifs au contrat d'assurances ;
• s'il y a lieu le responsable, les victimes ou leurs ayants droit, ainsi que leurs représentants ; les témoins, les tiers intéressés à l'exécution du contrat.

### *c. Les personnes bénéficiant d'un droit de communication :*

• Les autorités publiques dans le cadre de la sécurité publique ou de la défense nationale, des poursuites pénales ou à l'exécution des missions dont elles sont investies conformément aux lois et règlements en vigueur[30].
• Les autorités judiciaires;
• Les autorités de contrôle, l'association professionnelle des compagnies d'assurances et tous les organismes publics habilités ;
• Les structures chargées du contrôle et d'audit internes et externes.

## B. Les bénéficiaires spécifiques à certains traitements

### *a. Dans le cadre de la prospection commerciale*

**Peuvent, dans les limites de leurs attributions respectives, avoir accès aux données à caractère personnel**

• les personnes chargées du service marketing, du service commercial, des services chargés de traiter la relation client, les réclamations, et la prospection, des services informatiques ainsi que leurs responsables hiérarchiques ;

• les services chargés du contrôle (commissaire aux comptes, services chargés des procédures internes du contrôle...) ;
• les sous-traitants.

**Peuvent être destinataires des données:**

• les partenaires et sociétés extérieures (sociétés avec lesquelles l'entreprise entretient des relations commerciales régulières), les entités du groupe de sociétés ;
• les auxiliaires de justices, les officiers ministériels et organismes publics habilités à les recevoir, les arbitres, les médiateurs.

[30] Article 47 de la loi organique n°63 du 27 juillet 2004

### *b. Dans le cadre de la lutte contre la fraude*

**Aux fins de lutte contre la fraude interne:**

• les personnes habilitées de la direction des ressources humaines pour des requêtes ponctuelles et individuelles réalisés dans le cadre d'enquêtes internes consécutives à la détection d'une fraude ;
• le conseil de discipline saisi en cas de fraude ;
• les représentants du personnel dans le cadre de l'accompagnement d'un salarié mis en cause pour fraude.

Aux fins de lutte contre la fraude interne et externe :

• les personnels en relation avec la clientèle et les gestionnaires de contrats et de sinistres ;
• les autres entités d'un même groupe dès lors qu'elles sont concernées par la fraude ou interviennent dans la gestion des dossiers ou de maîtrise du risque de fraude ;
• les personnels habilités en charge de la lutte contre la fraude, de la lutte anti-blanchiment et du contrôle interne, les inspecteurs, enquêteurs, experts, et auditeurs ;
• le personnel habilité de la direction générale, la direction juridique et contentieux;
• le personnel habilité des sous-traitants. Dès lors qu'ils sont directement concernés par une suspicion de fraude, peuvent être destinataires des données relatives à cette fraude, les personnels habilités
• Les autres responsables de traitement intervenant dans le cadre des dossiers présentant une fraude ou suspicion de fraude : les autorités judiciaires et policières, les autres entreprises d'assurances, la FTUSA, le CGA et leurs personnels habilités.
• des organismes sociaux lorsque les régimes sociaux interviennent dans le règlement des sinistres ou lorsque les responsables de traitement offrent des garanties complémentaires à celles des régimes sociaux ;
• des organismes professionnels intervenant dans le cadre de dossiers présentant un risque de fraude pour les seules données concernées par ce dossier ;
• les auxiliaires de justice;
• l'autorité judiciaire, médiateur, arbitre saisis d'un litige ;
• les organismes tiers autorisés par une disposition légale à obtenir la communication de données à caractère personnel relatives à des précontentieux, contentieux ou condamnations ;
• s'il y a lieu les victimes de fraudes ou leurs représentants.

### *c. Dans le cadre de la lutte contre le blanchiment des capitaux et le financement du terrorisme et du respect des sanctions économiques et financières internationales*

**Parmi les responsables de traitement :**

• les personnes en relation avec la clientèle et les gestionnaires de contrats et de sinistres pour les clients dont ils ont la charge à l'exception des informations relatives aux déclarations de soupçon.
• les personnes habilitées à prendre la décision de nouer ou de maintenir une relation d'affaires avec une personne politiquement exposée (PPE).
• les personnels habilités du (ou des) service(s) chargé(s) de la lutte contre le blanchiment, notamment ceux ayant la qualité de correspondant ou suppléant CTAF, au sein de l'organisme responsable du traitement.

• les autres entités d'un même groupe dès lors qu'elles sont concernées par la lutte contre le blanchiment et le respect des sanctions économiques et financières internationales ou qu'elles interviennent dans la gestion des dossiers ou de maîtrise de ces risques

**Les autorités compétentes :**

• la CTAF et la CNLCT

• pour les données relatives aux personnes qui font l'objet d'une mesure de gel des avoirs, la Direction Générale du Trésor.

## 12. Les documents à élaborer par l'entreprise d'assurance

L'entreprise d'assurance est tenue d'élaborer un ensemble de documents nécessaires à la mise en conformité en matière de protection des données personnelles notamment ce qui suit :

- La charte/la politique de protection des données personnelles (cf annexe 6)
- Les conditions générales d'utilisation du site web (cf annexe 7)
- La charte et la politique des systèmes d'informations (s'orienter vers le responsable de sécurité des systèmes d'informations RSSI)

# Chapitre 5
## Les droits des personnes concernées

# 1. Le droit d'accès

## A. Définition du droit d'accès

Selon l'article 32[31], le droit d'accès concerne le droit de la personne concernée, de ses héritiers ou de son tuteur de consulter toutes les données à caractère personnel la concernant, ainsi que le droit de les corriger, compléter, rectifier, mettre à jour, modifier, clarifier ou effacer lorsqu'elles s'avèrent inexactes, équivoques, ou que leur traitement est interdit.

Le droit d'accès couvre également le droit d'obtenir une copie des données dans une langue claire et conforme au contenu des enregistrements, et sous une forme intelligible lorsqu'elles sont traitées à l'aide de procédés automatisés.

## B. Qui peut l'exercer ?

Le droit d'accès est exercé par la personne concernée, ses héritiers ou son tuteur à des intervalles raisonnables et de façon non excessive. (Article 34)

## C. La renonciation au droit d'accès

Selon l'article 33, on ne peut préalablement renoncer au droit d'accès ce qui en fait un droit d'ordre public ne pouvant être écarté même dans un contrat, loi des parties.

## D. Quelle limitation au droit d'accès ?

Selon l'article 35, la limitation du droit d'accès de la personne concernée, de ses héritiers ou de son tuteur aux données à caractère personnel la concernant n'est possible que dans les cas suivants :

- Lorsque le traitement des données à caractère personnel est effectué à des fins scientifiques et à condition que ces données n'affectent la vie privée de la personne concernée que d'une façon limitée ;
- Si le motif recherché par la limitation du droit d'accès est la protection de la personne concernée elle-même ou des tiers.

## E. Auprès de qui le droit d'accès est exercé ?

Lorsqu'il y a plusieurs responsables du traitement des données à caractère personnel ou lorsque le traitement est effectué par un sous-traitant, le droit d'accès est exercé auprès de chacun d'eux. (Article 36)

## F. Que peut demander la personne concernée ?

Selon l'article 40 la personne concernée, ses héritiers ou son tuteur peut suite à la demande d'accès demander du responsable de traitement ce qui suit :

- De rectifier les données à caractère personnel, les compléter, les modifier, les clarifier, les mettre à jour, les effacer lorsqu'elles s'avèrent inexactes, incomplètes, ou ambiguës,
- De détruire ces données lorsque leur collecte ou leur utilisation a été effectuée en violation de la loi en vigueur.

[31] Tous les articles de ce chapitre sont ceux de la loi organique n°2004-63 du 27 juillet 2004 portant sur la protection des données à caractère personnel

- De lui délivrer une copie des données à caractère personnel : la personne concernée peut demander, sans frais et après l'accomplissement des procédures requises et indiquer ce qui n'a pas été réalisé en ce qui concerne ces données.

## G. Comment est exercé le droit d'accès ?

Selon l'article 38, La demande d'accès est présentée par la personne concernée ou ses héritiers ou son tuteur par écrit ou par n'importe quel moyen laissant une trace écrite.
La personne concernée, ses héritiers ou son tuteur peuvent demander de la même manière l'obtention de copies des données dans un délai ne dépassant pas un mois à compter de ladite demande.

## H. L'obligation du responsable de traitement et du sous-traitant

Selon l'article 40, le responsable de traitement ou le sous-traitant doit lui délivrer une copie des données demandées dans un délai ne dépassant pas un mois à compter de la date de la sa demande.

## I. Les litiges pouvant naitre du droit d'accès

### *a. Les différents cas de litiges*

**Refus d'accès**
Le responsable du traitement ou le sous- traitant refuse de permettre à la personne concernée, à ses héritiers ou à son tuteur de :

- Consulter les données à caractère personnel requises,
- Différer l'accès à ces données,
- Délivrer une copie des données demandées (articles 38 et 40)

**La destruction/la dissimulation des données personnelles**
Le responsable de traitement ou le sous-traitant compte détruire ou dissimuler les données personnelles. (Article.38)

**Non-respect du délai**
Le responsable de traitement ou le sous-traitant ne respecte pas le délai d'un mois pour répondre à la demande de la personne concernée. (Article.40)

**Inexactitude des données**

Un litige sur l'exactitude des données à caractère personnel (Article.39)

### *b. Que faut-il faire en cas de litige ?*

**En cas de refus d'accès :**
La personne concernée, ses héritiers ou son tuteur peuvent présenter une demande à l'Instance dans un délai maximum d'un mois à compter de la date du refus.

**En cas de la destruction/la dissimulation des données**
La personne concernée, ses héritiers ou son tuteur peuvent présenter à l'Instance, le cas échéant, une demande afin de prendre toutes les mesures appropriées pour empêcher la destruction ou la dissimulation des données à caractère personnel.

### *c. Le rôle de l'INPDP en cas de litige*

**En cas de refus d'accès**
L'INPDP, après l'audition des deux parties et l'accomplissement des investigations nécessaires, peut ordonner la consultation des informations requises ou la délivrance d'une copie de ces informations ou l'approbation du refus, et ce, dans un délai ne dépassant pas un mois à compter de la date de sa saisine.

**En cas de la destruction des données personnelles**
L'INPDP doit statuer sur la demande dans un délai de sept jours à compter de la date de l'introduction de la demande.
La destruction ou la dissimulation de ces données est interdite dès la présentation de la demande.
D'une manière générale, l'INPDP est saisie de tout litige relatif à l'exercice du droit d'accès. Sous réserve des délais spécifiques prévus par la loi, l'INPDP doit rendre sa décision dans un délai d'un mois à compter de la date de sa saisine. (Article 41)

### *d. Que doit faire le responsable de traitement ou le sous-traitant en cas de litige sur l'exactitude des données ?*

En cas de litige sur l'exactitude des données à caractère personnel, le responsable du traitement et le sous-traitant **doivent mentionner l'existence de ce litige** jusqu'à ce qu'il y soit statué. (Article 39)

## 2. Le droit d'opposition

### A. Bénéficiaire du droit d'opposition

Selon l'article 42, le droit d'opposition peut être exercé par la personne concernée, ses héritiers ou son tuteur et ce à tout moment du traitement des données à caractère personnel le concernant.

### B. Exceptions à l'exercice du droit d'opposition

Le droit d'opposition ne peut pas être exercé par les personnes citées ci-dessus dans les cas où le traitement est **prévu par la loi** ou est exigé par **la nature de l'obligation contractuelle** qui lie les deux parties (Article 42).
Le droit d'opposition a été conditionné dans son exercice par la loi à des raisons valables, légitimes et sérieuses. Ces raisons sont ainsi évaluées par le responsable de traitement sous le contrôle de l'INPDP.

### C. Moment pour s'opposer

La personne concernée, ses héritiers ou son tuteur, a le droit de s'opposer à tout moment au traitement des données à caractère personnel le concernant pour des raisons valables, légitimes et sérieuses comme il a le droit de s'opposer à ce que les données à caractère personnel la concernant soient communiquées aux tiers en vue de les exploiter à des fins publicitaires (Article 42).

### D. Effets de l'opposition

L'opposition oblige le responsable de traitement de suspendre immédiatement le traitement des données personnelles.

## 3. Les autres droits

Selon la législation et la réglementation en vigueur, il y a une liste des droits qui découlent du droit d'accès[32] , on cite entre autres :

- Le droit de rectification (Correction ou mise à jour)
- Le droit d'effacement (Ecrasement des données)
- Le droit à l'oubli (Destruction ou anonymisation des données)

### A. Le droit de rectification :

Les personnes concernées ont le droit de demander que le responsable de traitement procède à la rectification des données à caractère personnel incomplètes ou incorrectes.
Le responsable du traitement est tenu de mettre à jour continuellement les données personnelles et les effacer si elles s'avèrent inexactes.
L'article 21 de la loi organique n° 2004-63 du 27 juillet 2004 portant sur la protection des données à caractère personnel dispose : «Le responsable du traitement et le sous-traitant doivent corriger, compléter, modifier ou mettre à jour les fichiers dont ils disposent, et effacer les données à caractère personnel de ces fichiers s'ils ont eu connaissance de l'inexactitude ou de l'insuffisance de ces données».
L'article 94 de la même loi organique prévoit qu'il est puni de trois mois d'emprisonnement et d'une amende de mille dinars quiconque viole les dispositions de cet article 21.

### B.Le droit à l'effacement ou le droit à l'oubli :

Les personnes concernées ont le droit de voir leurs données à caractère personnel définitivement effacées des bases de données d'une organisation particulière.
C'est un nouveau droit humain issu du recours massif aux technologies de l'information.
C'est le droit pour la personne concernée de voir ces données personnelles gardées pour un temps limité, celui nécessaire pour atteindre la finalité à la base de leur collecte.
L'article 45 de la loi organique n° 2004-63 du 27 juillet 2004 portant sur la protection des données à caractère personnel dispose : «Les données à caractère personnel doivent être détruites dès l'expiration du délai fixé à sa conservation dans la déclaration ou l'autorisation ou les lois spécifiques ou en cas de réalisation des finalités pour lesquelles elles ont été collectées ou lorsqu'elles deviennent inutiles pour l'activité du responsable du traitement».

[32] La loi tunisienne a englobé dans la section relative au droit d'accès (articles 32 à 41) un nombre plus large de droits qui sont les suivants :
- Droit de corriger (Articles 32 et 40)
- Droit de compléter (Articles 32 et 40)
- Droit de rectifier (Articles 32 et 40)
- Droit de mettre à jour (Articles 32 et 40)
- Droit de modifier (Articles 32 et 40)
- Droit de clarifier (Articles 32 et 40)
- Droit d'effacer (lorsque les données personnelles s'avèrent inexactes, incomplètes, ambiguës, équivoques, ou que leur traitement est interdit ou ne répond pas aux finalités indiquées) (Articles 32 et 40)
- Droit de détruire (lorsque leur collecte ou leur utilisation a été effectuée en violation de la présente loi) (Articles 40 et 45)
- Droit de porter plainte (Articles 38)

Les moyens techniques pour l'exercice des droits sont expliqués dans l'article 37[33] .

## 4. Les délais

### A. Pour le responsable de traitement ou le sous-traitant

Un mois pour répondre à la demande du bénéficiaire du droit d'accès.

### B. Pour la personne concernée, ses héritiers ou son tuteur

Un mois à compter de la date de refus pour porter plainte.
Sans délai précis dans le cas de destruction ou dissimulation.

### C. Pour l'INPDP

Un mois de la date de la saisine pour la réponse concernant le cas de refus ou tout autre litige relatif au droit d'accès et ce hors la destruction ou dissimulation.
Un mois de la date de la saisine pour la réponse en cas de litige relatif au droit d'opposition.
Sept jours de la date de la demande pour la réponse en cas de la destruction ou dissimulation.

## 5. En cas de litige

### A. Voie de recours

La personne concernée, ses héritiers ou son tuteur introduit une demande auprès de l'INPDP.

### B. Mission de l'INPDP

L'INPDP doit rendre sa décision dans un délai d'un mois (Articles 41 et 43).

### C. Si la personne concernée est un enfant

Le juge de la famille statue sur les litiges relatifs à l'opposition lorsque la personne concernée est un enfant.

[33] Le responsable du traitement automatisé des données à caractère personnel et le sous-traitant doivent mettre en œuvre les moyens techniques nécessaires pour permettre à la personne concernée, à ses héritiers ou à son tuteur l'envoi par voie électronique de sa demande de rectification, de modification, de correction, ou d'effacement des données à caractère personnel.

# LES ANNEXES

# Annexe 1
# Clause type de Protection des données personnelles du sous-traitant

Le sous-traitant s'engage à respecter la législation en vigueur en matière de protection des données à caractère personnel. Ainsi, il s'engage à traiter l'ensemble des données personnelles dont il a eu connaissance au titre de la /du présent(e)contrat/traité/ convention, dans le cadre strict et nécessaire des prestations à exécuter, et en tout état de cause, à n'agir que sur instructions écrites et préalables de la compagnie d'assurance et en conformité à ladite législation.

Le sous-traitant est tenu de prendre les diligences et moyens nécessaires pour garantir la confidentialité et la sécurité des données à caractère personnel qu'il pourrait traiter lors de l'exécution de ce/ cette contrat/traité/convention.

Il ne doit faire aucune copie des documents et supports relatifs aux données personnelles confiées autrement que dans le strict cadre de l'exécution de la /du présent(e)contrat/traité/convention.

La compagnie d'assurances se réserve le droit de prendre les mesures nécessaires en cas de manquement du sous-traitant à ses obligations pour la protection des données à caractère personnel.

Le sous-traitant reconnait que toute divulgation qui léserait les intérêts de la compagnie d'assurances donnera la possibilité à cette dernière d'engager des poursuites judiciaires à son encontre et réclamer des dommages et intérêts.

Le sous-traitant est tenu d'informer la compagnie d'assurances au cas où elle est soumise à une opération de contrôle de la part de l'instance de protection des données à caractère personnel et de lui communiquer un compte rendu sur l'opération.

La compagnie d'assurances peut décider la résiliation du/de la présent(e) contrat/ traité/ convention traité(e) s'il s'avère que le sous-traitant a failli à ses obligations en matière de protection des données personnelles.

# Annexe 2
# Modèle de mention d'informations

En application de la législation en vigueur en matière de protection des données à caractère personnel (Article 31 de la loi 63 de 2004), j'ai été informé(e):

- L'identité et les coordonnées du responsable de traitement (A indiquer)
- De la finalité du traitement (à indiquer clairement) de mes données qui sont des données personnelles indispensables et obligatoires pour la gestion et l'exécution du contrat d'assurances, la prospection et la gestion commerciale ainsi que tout autre traitement imposé par la législation en vigueur.

- De la nature des données personnelles (A indiquer) traitées dans le cadre du contrat.
- Le caractère obligatoire ou facultatif de la réponse et les conséquences de cela.
- Que les bénéficiaires de mes données sont la compagnie d'assurances et ses sous-traitants dans le cadre de l'exécution du contrat

- Que mes données à caractère personnel sont conservées aussi longtemps que nécessaire pendant la durée de vie de mon contrat et à la période postérieure pendant laquelle la conservation est nécessaire pour permettre le respect des obligations conformément aux délais de prescription et à toute autre disposition légale.

- Que la compagnie d'assurances et ses sous-traitants ont mis en place tous les moyens aptes à assurer la confidentialité et la sécurité de mes données à caractère personnel, de manière à empêcher leur endommagement, effacement ou accès par des tiers non autorisés et que l'accès à mes données à caractère personnel est strictement limité au personnel concerné de la compagnie d'assurances, le cas échéant, à ses sous-traitants qui sont soumis à une obligation de confidentialité et de protection des données personnelles.

- Que certains destinataires de mes données sont situés en dehors de la Tunisie notamment dans le cadre de la réassurance et de l'assistance internationale.

- De mes droits de s'opposer au traitement, d'accéder à mes données, et de mon droit de porter plainte auprès de l'INPDP contre toute violation constatée au cours de traitement de mes données personnelles.

- Mes droits peuvent être exercés à tout moment par simple demande à adresser par courrier électronique auprès des chargés de Protection des données personnelles de la compagnie à l'adresse mail : … ou par courrier postal à l'adresse …

# Annexe 3
# Engagement de confidentialité

Je soussigné(e) Monsieur/Madame _____, exerçant les fonctions de _____ au sein de l'Entreprise d'assurance…… (ci-après dénommé «la Société»), étant à ce titre amené à accéder à des données à caractère personnel, avoir en connaissance la confidentialité des dites données.

Je m'engage par conséquent, conformément au disposition de loi organique N°63/ 2004 portant sur la protection des données à caractère personnelle ainsi qu'à la politique de protection des données personnelle communiquée par l'Entreprise d'Assurance, à prendre toutes précautions conformes aux procédures dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient modifiées, endommagées ou communiquées à des personnes non expressément autorisées à les recevoir.

Je m'engage en particulier à :

- Ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions;
- Ne faire aucune copie de ces données sauf si cela est nécessaire à l'exécution de mes attributions ;
- Prendre toutes les mesures conformes aux procédures dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- Prendre toutes précautions conformes aux procédures pour préserver la sécurité matérielle de ces données;
- M'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- Restituer intégralement les fichiers informatiques et tout support d'information relatif à ces données en cas de cessation de mes fonctions,

**J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénale conformément au décret-loi n°2022-54 en date du 13 septembre 2022 relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication.**

Cet engagement de confidentialité, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause.

Fait à _____ le_____

Nom :

Signature :

# Annexe 4
# Le modèle du formulaire d'exercice des droits de Protection des données personnelles

Ce formulaire, mis en place conformément à la législation et la réglementation en vigueur en matière de PDP, vous permet de d'exercer vos droits sur les Données Personnelles demander des informations sur les traitements de vos Données Personnelles gérées par l'entreprise d'assurances ou vous concernant faisant l'objet de ces traitements. Il doit être retourné signé à l'adresse : ----------, ou par mail à : dpo@

## 1-identification du demandeur

☐ Monsieur ☐ Madame

Nom * : Prénom * : Email * :

Téléphone * :

Adresse Postale :

Numéro de la pièce d'identité :

Profil du demandeur (Client, Employé, assuré, bénéficière, victime …) :

Numéro de contrat ou sinistre :

## 2-Droit objet de la demande *

En application de la législation et réglementation en vigueur relatif à la protection des données à Caractère Personnel, je souhaite faire valoir :

1 - Droit d'accès ☐
2 - Droit d'opposition ☐
3 - Droit de rectification ☐
4 - Droit d'effacement ☐
5 - Droit à l'oubli ☐
6 - Droit de retrait du consentement ☐
7 - Autre demande : ☐

### 3-Description de la demande *

### 4- justificatif d'identité à joindre *

☐ Je m'engage à communiquer, en complément de ce formulaire, une copie d'une pièce d'identité permettant au Responsable de Traitement de m'authentifier formellement[34] (excepté pour la demande d'opposition au traitement à des fins de prospection commerciale précontractuelle).

☐ En cochant cette case, je donne mon consentement[35] pour le recueil et le traitement des Données Personnelles renseignées dans ce formulaire

Les informations recueillies à partir de ce formulaire permettent le traitement de votre demande et ne seront conservées qu'en cas de besoin impérieux de preuve. Elles sont enregistrées et transmises aux services concernés par votre demande.

L'entreprise d'assurance se réserve le droit de vous contacter afin de demander des informations ou documents supplémentaires nécessaires au traitement de votre demande.

Fait à : Date :

Signature

* Rubrique à renseignement obligatoire

[34] Le formulaire non accompagné du justificatif d'identité ne pourrait pas été traité par l'entreprise d'assurance CIN recto-verso, Passeport, titre de séjour

[35] Le consentement concerne les personnes physiques n'ayant aucune relation contractuelle avec l'entreprise d'assurances

# Annexe 5
# Fiche de cartographie modèle de l'INPDP

**MODELE DE FICHE A RENSEIGNER POUR CHAQUE TRAITEMENT DE DONNES PERSONNELES**

Etablir une fiche pour chaque traitement de données ayant une finalité distinctive

| | |
|---|---|
| Référence du traitement ( à attribuer en interne) | |
| Nom et adresse du responsable de traitement | |
| Date de mise en œuvre | |
| Finalité principale ( But ) | |
| Détails des finalités de traitement | |
| Service chargé du traitement | |
| Personne ou service chargé du droit d'accès | |
| Catégories des personnes concernées par le traitement | |
| Données traitées | |
| Localisation de l'hébergement des données | |
| Destinataires des données au national et base légal | |
| Destinataires des données au international et base légal | |
| Durée de conservation des données | |
| Date audit de sécurité | |
| Date de déclaration ou demande d'autorisation INPDP | |

# Annexe 6
# Registre de traitement

Le registre devrait comporter pour chaque finalité de traitement les données suivantes:

| Identification du traitement | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Nom | Référence | Date de début | Date de fin | Date mise à jour | Date déclaration | Référence déclaration | Date demande d'autorisation | Référence autorisation | Service ou département |

| | | | | | |
|---|---|---|---|---|---|
| Finalité du traitement | Sous-finalité | Détails de la finalité | Base légale de traitement | Type de traitement | Outils de traitement |

| Donnée(s) et sujet(s) de donnée(s) utilisée(s) | | | |
|---|---|---|---|
| Personne(s) concernée(s) | Catégorie de données | Durée de conservation | Mesures pour la destruction |

| Acteurs |
|---|
| |

| Destinataires |
|---|
| |

| Accès | |
|---|---|
| Personnes habilitées à y accéder | |

| Hébergement et stockage | |
|---|---|
| Interne | Externe |

| Transfert hors la Tunisie | | | | |
|---|---|---|---|---|
| Catégorie de données transférées | Bénéficiaire | Pays tiers | Les garanties appropriées | Technologies |

| Risques et mesures d'atténuation | |
|---|---|
| Risques | Description des mesures d'atténuations |

| Droit(s) de personne(s) concernée(s) | | |
|---|---|---|
| Droit de personne(s) concernée(s) | Procédures d'exercice des droits | Commentaires |

# Annexe 7
# La charte interne de protection des données personnelles

Nous, l'entreprise d'assurances _____, attachons une haute importance à la protection de vos données personnelles et faisons-en sorte que vous vous sentiez en sécurité lors de l'utilisation de nos services ainsi que de notre site web. Nous respectons votre vie privée et nous nous engageons à respecter et protéger vos données personnelles. Nous veillons ainsi à adopter et à respecter rigoureusement une politique de protection des données personnelles conforme à la législation et réglementation en vigueur.

## Champ d'application

La présente charte s'applique à tous les traitements de données au sein de notre Entreprise d'assurances, au niveau de nos succursales et agences et sur le site web. Nous nous engageons également à relayer ces engagements auprès de nos sous-traitants et partenaires.

## Définitions

**Données personnelles :** toutes les informations quelle que soit leur origine ou leur forme et qui permettent directement ou indirectement à identifier une personne physique ou la rendent identifiable (nom, prénom, N° CIN/Passeport, adresse, e-mail, son, l'image etc… y compris le son et l'image) à l'exception des informations liées à la vie publique ou considérées comme telles par la législation en vigueur.

**Traitement de données à caractère personnel.** Les opérations réalisées d'une façon automatisée ou manuelle par une personne physique ou morale, et qui ont pour but notamment la collecte, l'enregistrement, la conservation, l'organisation, la modification, l'exploitation, l'utilisation, l'expédition, la distribution, la diffusion ou la destruction ou la consultation des données à caractère personnel, ainsi que toutes les opérations relatives à l'exploitation de bases des données, des index, des répertoires, des fichiers, ou l'interconnexion.

**Responsable du traitement.** Toute personne physique ou morale qui détermine les finalités et les moyens du traitement des données à caractère personnel.

## Responsable de traitement des données à caractère personnel

Le responsable du traitement de vos données à caractère personnel est l'entreprise d'assurances... ayant pour identifiant unique..., dont le siège social est situé à ...

## Nos principes

- Licéité, Loyauté et transparence : les données personnelles sont traitées de manière licite, -loyale et transparente.
- Limitation des finalités : les données personnelles sont collectées pour des finalités déterminées, explicites et légitimes.
- Minimisation des données : les données personnelles sont conservées de manière adéquate, pertinente et sont limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

• Exactitude : les données personnelles sont exactes, tenues à jour et toutes les mesures raisonnables sont prises pour que les données inexactes soient effacées ou rectifiées sans tarder.
• Limitation de la conservation : les données personnelles sont traitées en limitant la durée de conservation par rapport à la finalité.
• Intégrité et confidentialité : les données personnelles sont traitées de façon à garantir une sécurité appropriée via la mise en œuvre des moyens adéquats.

### Finalités de la collecte de vos données

Les données personnelles traitées ont pour objectif de répondre à une ou plusieurs finalités définies par l'entreprise d'assurances.

### Sécurité

Nous vous informons que nous prenons toutes les précautions utiles, mesures organisationnelles et techniques appropriées pour préserver la sécurité, l'intégrité et la confidentialité de vos données à caractère personnel et notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

### Consentement

Chaque fois qu'il est nécessaire, vous pouvez donner expressément votre consentement pour le traitement de vos données personnelles.

### Protection des données à caractère personnel communiquées sur le site WEB

Les informations recueillies sur le site … font l'objet d'un traitement destiné principalement :
• À l'établissement d'un devis
• Au dépôt de candidature spontanée
• À l'envoi de newsletters
• À l'envoi d'une réclamation…

Ces données seront traitées par les services compétents de la Compagnie conformément à la législation et la réglementation en vigueur.

### Utilisation de «Cookies»

Les cookies sont de petits fichiers texte envoyés sur votre ordinateur afin que nos sites Web se souviennent de vos paramètres et des informations que vous avez saisies, de sorte que vous n'ayez pas besoin de les saisir à nouveau lorsque vous retournez vers une page ou que vous ouvrez une nouvelle page de navigation. Nous utilisons également les Cookies pour analyser comment vous consultez nos sites Web afin de s'assurer qu'ils répondent à vos besoins. Vous pouvez décider d'autoriser ou de bloquer les Cookies sur votre ordinateur.

### Mise à jour de la présente charte

Cette charte peut être modifiée et enrichie, nous nous engageons à la faire évoluer en fonction de vos attentes dans la limite des dispositions légales et réglementaires.

# Annexe 8
# Conditions générales d'utilisation du site web

Le présent document a pour objet de définir les modalités et conditions dans lesquelles d'une part, l'Entreprise d'Assurances ____ , ci-après dénommée l'EDITEUR, met à la disposition de ses utilisateurs le site, et les services disponibles sur le site et d'autre part, la manière par laquelle l'utilisateur accède au site et utilise ses services.
Toute connexion au site est subordonnée au respect des présentes conditions.
Pour l'utilisateur, le simple accès au site de l'EDITEUR à l'adresse URL suivante ……____ implique l'acceptation de l'ensemble des conditions décrites ci-après.

**Propriété intellectuelle**

*Variante 1*
La structure générale du site ____ , ainsi que les textes, graphiques, images, sons et vidéos la composant, sont la propriété de l'éditeur ou de ses partenaires. Toute représentation et/ou reproduction et/ou exploitation partielle ou totale des contenus et services proposés par le site ____ , par quelque procédé que ce soit, sans l'autorisation préalable et par écrit de l'EDITEUR et/ou de ses partenaires est strictement interdite et serait susceptible de constituer une contrefaçon.

Variante 2
Aucune reproduction, même partielle, ne peut être faite de ce site sans l'autorisation de l'EDITEUR.

Variante 3
Tous les éléments de ce site, y compris les documents téléchargeables, sont libres de droit. A l'exception de l'iconographie, la reproduction des pages de ce site est autorisée à la condition d'y mentionner la source. Elles ne peuvent être utilisées à des fins commerciales et publicitaires.

**Liens hypertextes**
Le site ____ peut contenir des liens hypertextes vers d'autres sites présents sur le réseau Internet. Les liens vers ces autres ressources vous font quitter le site
Il est possible de créer un lien vers la page de présentation de ce site sans autorisation expresse de l'EDITEUR. Aucune autorisation ou demande d'information préalable ne peut être exigée par l'éditeur à l'égard d'un site qui souhaite établir un lien vers le site de l'éditeur. Il convient toutefois d'afficher ce site dans une nouvelle fenêtre du navigateur. Cependant, l'EDITEUR se réserve le droit de demander la suppression d'un lien qu'il estime non conforme à l'objet du site

**Responsabilité de l'éditeur**
Les informations et/ou documents figurant sur ce site et/ou accessibles par ce site proviennent de sources considérées comme étant fiables.
Toutefois, ces informations et/ou documents sont susceptibles de contenir des inexactitudes techniques et des erreurs typographiques.
L'EDITEUR se réserve le droit de les corriger, dès que ces erreurs sont portées à sa connaissance.
Il est fortement recommandé de vérifier l'exactitude et la pertinence des informations et/ou documents mis à disposition sur ce site.
Les informations et/ou documents disponibles sur ce site sont susceptibles d'être modifiés à tout moment,

et peuvent avoir fait l'objet de mises à jour. En particulier, ils peuvent avoir fait l'objet d'une mise à jour entre le moment de leur téléchargement et celui où l'utilisateur en prend connaissance.
L'utilisation des informations et/ou documents disponibles sur ce site se fait sous l'entière et seule responsabilité de l'utilisateur, qui assume la totalité des conséquences pouvant en découler, sans que l'EDITEUR puisse être recherché à ce titre, et sans recours contre ce dernier.
L'EDITEUR ne pourra en aucun cas être tenu responsable de tout dommage de quelque nature qu'il soit résultant de l'interprétation ou de l'utilisation des informations et/ou documents disponibles sur ce site.

**Accès au site**
L'éditeur s'efforce de permettre l'accès au site 24 heures sur 24, 7 jours sur 7, sauf en cas de force majeure ou d'un événement hors du contrôle de l'EDITEUR, et sous réserve des éventuelles pannes et interventions de maintenance nécessaires au bon fonctionnement du site et des services.

Par conséquent, l'EDITEUR ne peut garantir une disponibilité du site et/ou des services, une fiabilité des transmissions et des performances en terme de temps de réponse ou de qualité. Il n'est prévu aucune assistance technique vis à vis de l'utilisateur que ce soit par des moyens électronique ou téléphonique.

La responsabilité de l'éditeur ne saurait être engagée en cas d'impossibilité d'accès à ce site et/ou d'utilisation des services.

Par ailleurs, l'EDITEUR peut être amené à interrompre le site ou une partie des services, à tout moment sans préavis, le tout sans droit à indemnités. L'utilisateur reconnaît et accepte que l'EDITEUR ne soit pas responsable des interruptions, et des conséquences qui peuvent en découler pour l'utilisateur ou tout tiers.

**Modification des conditions d'utilisation**
L'EDITEUR se réserve la possibilité de modifier, à tout moment et sans préavis, les présentes conditions d'utilisation afin de les adapter aux évolutions du site et/ou de son exploitation.

**Règles d'usage d'Internet**
L'utilisateur déclare accepter les caractéristiques et les limites d'Internet, et notamment reconnaît que :
L'EDITEUR n'assume aucune responsabilité sur les services accessibles par Internet et n'exerce aucun contrôle de quelque forme que ce soit sur la nature et les caractéristiques des données qui pourraient transiter par l'intermédiaire de son centre serveur.
L'utilisateur reconnaît que les données circulant sur Internet ne sont pas protégées notamment contre les détournements éventuels. La présence du logo  institue une présomption simple de validité. La communication de toute information jugée par l'utilisateur de nature sensible ou confidentielle se fait à ses risques et périls.
L'utilisateur reconnaît que les données circulant sur Internet peuvent être réglementées en termes d'usage ou être protégées par un droit de propriété.
L'utilisateur est seul responsable de l'usage des données qu'il consulte, interroge et transfère sur Internet.
L'utilisateur reconnaît que l'EDITEUR ne dispose d'aucun moyen de contrôle sur le contenu des services accessibles sur Internet

**Droit applicable**

Tant le présent site que les modalités et conditions de son utilisation sont régis par le droit tunisien, quel que soit le lieu d'utilisation. En cas de contestation éventuelle, et après l'échec de toute tentative de recherche d'une solution amiable, les tribunaux de Tunis seront seuls compétents pour connaître de ce litige.

Pour toute question relative aux présentes conditions d'utilisation du site, vous pouvez nous écrire à l'adresse suivante :……

# Annexe 9
# Recueil des textes relatifs à la Protection des données personnelles

## La constitution
## الدستور

دستور الجمهورية التونسية

## نصوص حماية المعطيات الشخصية
## Les normes de protection des données personnelles

2- قانون أساسي عدد63 يتعلق بحماية المعطيات الشخصية، 27 جويلية 2004

Loi organique numéro 63 en date du 27 juillet 2004 portant sur la protection des données à caractère personnel

3- أمر عدد3003 لسنة 2007 مؤرخ في 27 نوفمبر يتعلق بضبط طرق سير الهيئة الوطنية لحماية المعطيات الشخصية

Décret n° 2007-3003 du 27 novembre 2007, fixant les modalités de fonctionnement de l'instance nationale de protection des données à caractère personnel

4- التصريح والترخيص لمعالجة المعطيات الشخصية أمر عدد 3004 لسنة 2007 مؤرخ في 27 نوفمبر 2007 يتعلق بضبط شروط وإجراءات

Décret n° 2007-3004 du 27 novembre 2007, fixant les conditions et les procédures de déclaration et d'autorisation pour le traitement des données à caractère personnel

5- قانون أساسي عدد 42 لسنة 2017 مؤرخ في 30 ماي 2017 يتعلق بالموافقة على انضمام الجمهورية التونسية إلى الاتفاقية رقم 108 لمجلس أوروبا المتعلقة بحماية الأشخاص تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي وبروتوكولها الإضافي رقم 181 الخاص بسلطات المراقبة وانسياب وتدفق المعطيات عبر الحدود

Loi organique n° 2017-42 du 30 mai 2017, portant approbation de l'adhésion de la République Tunisienne à la convention n° 108 du conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de son protocole additionnel n° 181 concernant les autorités de contrôle et les flux transfrontières de données

6- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel consolidée à la lumière du protocole additionnel (Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, adopté par le Comité des Ministres
7- lors de sa 128e session à Elseneur, le 18 mai 2018) signée par la Tunisie en mai 2019

## قرارات الهيئة الوطنية
## Les délibérations de l'Instance nationale

8- قرار عدد 2 بتاريخ 6 أكتوبر 2017 يتعلق بالقواعد السلوكية الخاصة بمعالجة المعطيات الشخصية في نطاق العمل السياسي

9- قرار عدد 3 بتاريخ 5 سبتمبر 2018 يتعلق بتحديد الدول التي توفر حماية كافية وملائمة في المجال المتعلق بحماية المعطيات الشخصية

10- قرار عدد 4 بتاريخ 5 سبتمبر 2018 يتعلق بمعالجة المعطيات الشخصية المتعلقة بالصحة

11- قرار عدد 5 بتاريخ 5 سبتمبر 2018 يتعلق بضبط شروط وإجراءات تركيز وسائل المراقبة البصرية

12- قرار عدد 6 بتاريخ 2 جويلية 2019 يتعلق بأعمال الرقابة التي تقوم بها الهيئة الوطنية لحماية المعطيات الشخصية

## Les circulaires du Chef du Gouvernement
## مناشر رئيس الحكومة

13- منشور رئيس الحكومة عدد 17 بتاريخ 12 أكتوبر 2016
- Circulaire du Chef du Gouvernement 17 du 12 octobre 2016

14- منشور رئيس الحكومة عدد 8 بتاريخ 25 فيفر ي 2019
Circulaire du Chef du Gouvernement 8 du 25 février 2019

15- منشور رئيس الحكومة عدد 23 بتاريخ 5 نوفمبر 2019
Circulaire du Chef du Gouvernement 23 du 5 novembre 2019

## القوانين القطاعية
## Les lois sectorielles

16- قانو ن أساسي عدد 26 لسنة 2015 مؤرخ في 7 أوت 2015 يتعلق بمكافحة الإرهاب ومنع غسل الأموال
Loi organique n° 2015-26 du 7 août 2015, relative à la lutte contre le terrorisme et la répression du blanchiment d'argent

17- قانون أساسي عدد 22 لسنة 2016 مؤرخ في 24 مارس 2016 يتعلق بالحق في النفاذ إلى المعلومة
Loi organique n° 2016-22 du 24 mars 2016, relative au droit d'accès à l'information

18- قانو ن عدد 48 لسنة 2016 مؤرخ في 11 جويلية 2016 يتعلق بالبنوك والمؤسسات المالية
Loi n° 2016-48 du 11 juillet 2016, relative aux banques et aux établissements financiers

19- مرسوم من رئيس الحكومة عدد 17 لسنة 2020 مؤرخ في 12 ماي 2020 يتعلق بالمعرف الوحيد للمواطن
Décret-loi du Chef du Gouvernement n° 2020-17 du 12 mai 2020, relatif à l'identifiant unique du citoyen

20- أمر حكومي عدد 312 لسنة 2020 مؤرخ في 15 ماي 2020 يتعلق بضبط محتوى المعرف الوحيد للمواطن ومواصفاته الفنية وقواعد مسك سجله والتصرف فيه
Décret Gouvernemental n° 2020-312 du 15 mai 2020, fixant le contenu et les spécifications techniques de l'identifiant unique citoyen et les règles régissant la tenue et la gestion de son Registre

21- مرسوم من رئيس الحكومة عدد 31 لسنة 2020 مؤرخ في 10 جوان 2020 يتعلق بالتبادل الإلكتروني للمعطيات بين الهياكل والمتعاملين معها وفيما بين الهياكل
Décret-loi du Chef du Gouvernement n° 2020-31 du 10 juin 2020, relatif à l'échange électronique des données entre les structures et leurs usagers et entre les structures

## قرار الهيئة الوقتية لمراقبة دستورية مشاريع القوانين
## Décision de l'Instance provisoire de contrôle de constitutionnalité des projets de loi

22- أمر عدد 412 لسنة 2014 مؤرخ في 16 جانفي 2014 يتعلق بضبط شروط وإجراءات إسناد ترخيص لممارسة نشاط مشغل شبكة افتراضية للاتصالات
Décret n° 2014-412 du 16 janvier 2014, fixant les conditions et les procédures d'octroi de l'autorisation pour l'exercice de l'activité d'opérateur d'un réseau virtuel des télécommunications

23- قرار من وزير تكنولوجيات الاتصال والاقتصاد الرقمي مؤرخ في 10 سبتمبر 2018 يتعلق بضبط شروط تركيز واستغلال الشبكات العمومية لتراسل المعطيات WiFi ذات الاستعمال الخارجي
Arrêté du ministre des technologies de la communication et de l'économie numérique du 10 septembre 2018, fixant les conditions d'installation et d'exploitation des réseaux publics de transmission des données WiFi outdoor

## مشروع القانون المتعلق بحماية المعطيات الشخصية

Projet de loi organique relatif à la protection des données à caractère personnel dans la version soumise par le Gouvernement suite au conseil des ministres du 8 mars 2018

## احصائيات متعلقة بنشاط الهيئة

Statistiques relatives à l'activité de l'Instance

## معلقات متعلقة بحماية المعطيات الشخصية

Planches relatives à la protection des données personnelles

## خارطة العالم لحماية المعطيات الشخصية

La carte du monde de la protection des données personnelles.

## تراتيب ومقررات الهيئة العامة للتأمين

- الترتيب عدد 02 لسنة 2019 المؤرخ في 28 أوت 2019 حول تدابير العناية الواجبة المتعلّقة بمكافحة تمويل الإرهاب وانتشار التسلح ومنع غسل الأموال لدى قطاع التأمين.
- Règlement n°2 du 28 Aout 2019 relatif aux mesures de vigilance requises en matière de Lutte contre le Financement du Terrorisme et de prolifération des armes et la répression du blanchiment d'argent dans le secteur des assurances.
- مقرر عدد 01 مؤرخ في 13 جويلية 2016 يتعلق بضبط قواعد حسن الإدارة والتسيير بمؤسسات التأمين ومؤسسات اعادة التأمين
- Décision CGA n° 01/2016 du 13 Juillet 2016 fixant les règles de la bonne gouvernance et de gestion dans les sociétés d'assurance et de réassurance