



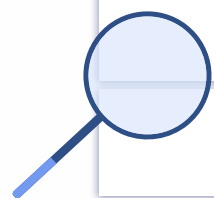
**FACS OCCITANIE**

Fédération des Acteurs de la Coordination en Santé

# Premiers pas vers la conformité RGPD accompagnée

Guide pratique à destination des adhérents

Un guide pour comprendre les enjeux,  
adopter les bons réflexes et s'orienter  
dans la mise en conformité, avec  
l'appui possible d'un DPO mutualisé.



# Mode d'emploi du guide

Ce guide propose deux niveaux de lecture pour s'adapter aux besoins de chacun. Le texte principal donne les **repères essentiels** pour comprendre progressivement les enjeux du RGPD.



Les encarts pratiques apportent des repères directement utilisables au quotidien :

- bons réflexes,
- points de vigilance,
- exemples concrets
- éléments de méthode.

## Exemples concrets



Ils peuvent également servir de support pour des échanges en équipe ou des temps de sensibilisation, notamment avec le relais RGPD ou le DPO. Ils constituent des repères d'action concrets, à mobiliser dans les pratiques quotidiennes.

## Bon réflexe



Pour une première lecture, les titres et les encarts suffisent pour avoir les repères essentiels. Pour approfondir ou structurer une démarche, il est possible de revenir sur les contenus complets et de s'appuyer sur un DPO lorsque la situation le nécessite.

# INTRODUCTION

## PREAMBULE

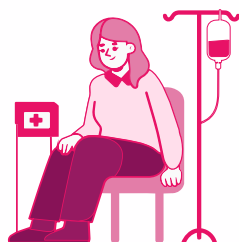
**Les structures adhérentes manipulent chaque jour des informations relatives à des personnes :** usagers, bénéficiaires, patients, familles, professionnels, partenaires ou salariés, dans des contextes parfois sensibles.



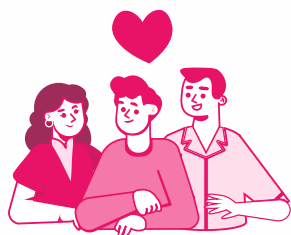
usagers



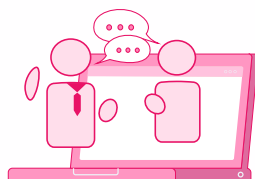
bénéficiaires



patients



familles



professionnels



partenaires  
ou salariés

Ces informations peuvent être utiles, parfois indispensables, mais elles doivent être utilisées avec précaution. **Dès qu'une information permet d'identifier une personne, directement ou indirectement**, elle devient une donnée personnelle et entre dans le champ du RGPD.

Ce règlement n'a pas pour objectif de complexifier le travail quotidien. Il vise à protéger les personnes, à éviter les erreurs fréquentes, et à instaurer des règles claires sur la manière dont les données sont collectées, utilisées, partagées, conservées et sécurisées.

Ce guide a pour objectif de donner des repères simples pour démarrer une démarche de conformité.

Il ne remplace pas une analyse complète ni un accompagnement adapté. Certaines situations nécessitent l'appui d'un Délégué à la Protection des Données (DPO), notamment dans les structures traitant des données sensibles.

Les bonnes pratiques présentées dans ce guide s'appuient sur les recommandations de la CNIL et visent à faciliter leur mise en œuvre concrète au quotidien.

## Point d'attention

Le guide permet de comprendre et d'identifier les enjeux. Pour certaines situations ou en cas de doute, un appui ponctuel du relais RGPD ou du DPO peut être utile afin d'analyser les situations, aider à prioriser les actions, sécuriser les pratiques et accompagner la démarche dans la durée.



# I. Pourquoi le RGPD concerne votre structure ?

Le RGPD s'applique dès qu'une structure collecte ou utilise des données personnelles, quel que soit le support :

logiciel

fichier Excel

email

dossier papier



Dans vos activités, cela concerne par exemple, à la gestion des usagers ou patients, les dossiers d'accompagnement, les échanges avec les partenaires, les ressources humaines et les actions de coordination.

## Bon réflexe

Avant de créer ou partager une information, posez-vous les 4 questions suivantes :

- Pourquoi cette donnée est-elle nécessaire ?
- Qui y a accès ?
- Combien de temps doit-elle être conservée ?
- Est-elle suffisamment protégée ?



## Le RGPD repose sur une idée simple :

les données personnelles doivent servir un **objectif clair et légitime**, être **connues des personnes concernées**, **rester sécurisées avec des accès maîtrisés**, et être **conservées uniquement le temps nécessaire**.

Le relais RGPD est le point de contact interne. Le DPO intervient en appui pour les situations nécessitant une analyse ou une sécurisation spécifique.

## Réflexe DPO



En cas de doute, de nouveau traitement, de partage de données ou d'incident, rapprochez-vous de votre relais RGPD ou du DPO pour sécuriser la situation.

## II. Comprendre ce qu'est une donnée personnelle

### Données personnelles

Une donnée personnelle est toute information permettant d'identifier une personne, directement ou indirectement.

Elle peut identifier une personne directement (nom, prénom, email nominatif, numéro de téléphone) ou indirectement (numéro de dossier, combinaison d'informations, situation particulière, identifiant interne).

Même sans le nom, une personne peut être identifiable si les informations permettent de la reconnaître par recoupement.

### Exemples concrets

Sont des données personnelles : identité, coordonnées, informations d'accompagnement, données de santé, données sociales, informations RH.

### Données sensibles

Certaines données nécessitent une vigilance renforcée. Les données sensibles sont des informations particulièrement protégées.

Elles peuvent concerner notamment la santé, le handicap, l'origine supposée, les opinions, les convictions, la vie ou l'orientation sexuelle ou certaines données biométriques.

Dans le secteur social, médico-social ou sanitaire, les données de santé et les données relatives à la situation sociale doivent être manipulées avec une grande prudence.

### Point d'attention

Supprimer le nom ou remplacer une identité par un numéro ne suffit pas toujours à anonymiser une donnée. Les données restent alors soumises au RGPD.



### Repère - Donnée anonymisée et pseudonymisée

#### **Donnée anonymisée :**

la personne ne peut plus être identifiée, même par recoupement. La donnée sort en principe du champ du RGPD.

#### **Donnée pseudonymisée :**

les identifiants directs sont remplacés par un code ou un numéro, mais la personne peut encore être réidentifiée grâce à une information de correspondance. La donnée reste donc une donnée personnelle soumise au RGPD.

# III. Identifier les usages de données personnelles

Le RGPD utilise le terme « traitement » pour désigner toute action réalisée sur des données personnelles. Il y a traitement dès qu'on collecte, utilise, consulte, modifie, classe, transmet, archive ou supprime des données. Cela concerne aussi bien les logiciels métiers que les tableaux de suivi, les dossiers papier, les emails ou une liste d'envoi.

## Exemples concrets

Les traitements les plus fréquents concernent le suivi des usagers ou patients, la gestion des rendez-vous, les ressources humaines (recrutement, formation), la facturation, la communication avec les familles ou partenaires, ainsi que la gestion de fichiers, de documents et des demandes des personnes.



### Point d'attention

Créer un fichier de suivi "à côté" (Excel, notes...) sans vérifier s'il existe déjà un outil prévu

Cela peut entraîner des doublons, des erreurs ou des oublis.

## Où se trouvent les données ?

Les données ne sont pas uniquement dans les logiciels métiers. On les retrouve aussi dans les dossiers papier, fichiers Excel, documents Word, emails, messageries, agendas partagés, outils collaboratifs, espaces cloud ou encore archives.

### Bon réflexe



Avant de créer un nouveau fichier de suivi, vérifiez s'il existe déjà un outil adapté. Les fichiers parallèles sont souvent pratiques à court terme, mais ils peuvent créer des risques : données en doublon, accès trop larges, conservation non maîtrisée ou difficulté en cas de demande ou d'incident.

### Point d'attention

Les fichiers Excel, tableaux de suivi et dossiers partagés sont souvent les plus sensibles car ils échappent facilement au contrôle. Ils doivent être identifiés, sécurisés et régulièrement revus.



## IV. Dresser un inventaire simple de ses traitements

Un recensement simplifié permet de mieux comprendre comment les données sont utilisées dans la structure.

L'objectif n'est pas de produire une documentation complexe, mais d'identifier les principaux usages : quelles données sont utilisées, pour qui, par qui, sur quels outils, et avec quels niveaux de partage et de risque.

Ce travail peut être affiné avec le DPO notamment pour repérer des doublons, vérifier les durées de conservation les accès et les partages.

| Question             | Exemple de réponse                                                           |
|----------------------|------------------------------------------------------------------------------|
| Objectif             | Organiser le suivi des personnes accompagnées                                |
| Personnes concernées | Usagers, familles, professionnels référents                                  |
| Données utilisées    | Identité, coordonnées, situation, historique des échanges, éléments de suivi |
| Support              | Logiciel métier et fichier de suivi interne                                  |
| Accès                | Équipe concernée, responsable de service                                     |
| Partage              | Partenaires habilités selon la situation                                     |
| Durée                | À définir avec le DPO selon les obligations applicables                      |
| Risques              | Accès trop large, commentaires inadaptés, erreur de destinataire             |
| Action à prévoir     | Vérifier les accès, limiter les commentaires, sécuriser les transmissions    |

### Point d'attention

L'inventaire ne concerne pas uniquement les logiciels métiers. Il doit aussi inclure les fichiers Excel, dossiers partagés, formulaires, listes de diffusion et outils de communication utilisés au quotidien.



# V. Comprendre les bases légales

Pour utiliser des données personnelles, il faut une **raison légitime** prévue par le RGPD. C'est ce qu'on appelle une **base légale**.

Elle permet de **justifier pourquoi la structure a le droit d'utiliser certaines données**. Elle doit être choisie **avant de commencer un traitement** et correspondre à l'**objectif poursuivi**.

Le choix de la base légale dépend du **contexte**, du **type de données**, de la **mission de la structure** et de la **relation avec la personne concernée**.



## Point d'attention

Le choix de la base légale peut être complexe selon les situations.

En cas de doute, il est recommandé de se rapprocher du relais RGPD ou du DPO.

## Réflexe DPO

Sollicitez le DPO avant de lancer un nouvel usage de données, en particulier si les données sont sensibles, si les personnes sont vulnérables, si plusieurs partenaires accèdent aux données ou si un outil numérique externe est utilisé.



## Repère - Les principales bases légales à connaître

- **L'obligation légale** : la structure traite les données parce qu'un texte l'y oblige. *Exemple : conserver certaines informations liées à la gestion des salariés, à la paie ou à la comptabilité.*
- **Le contrat** : les données sont nécessaires pour exécuter un contrat ou préparer sa mise en place. *Exemple : gérer une relation avec un salarié, un prestataire, ou un fournisseur.*
- **La mission d'intérêt public** : La structure traite des données dans le cadre de ses missions institutionnelles. *Exemple : accompagner les usagers dans un cadre réglementaire ou conventionnel.*
- **L'intérêt légitime** : la structure poursuit un intérêt réel et légitime à traiter des données, à condition que cela ne porte pas atteinte aux droits des personnes. *Exemple : sécuriser les locaux, organiser certains échanges professionnels ou gérer des relances internes proportionnées.*
- **Le consentement** : La personne accepte clairement et librement l'utilisation de ses données pour un usage précis. *Exemple : inscription volontaire à une lettre d'information.*

# VI. Sécuriser les données au quotidien

La sécurité des données repose sur des **outils**, mais aussi sur des **habitudes de travail**.

La plupart des incidents viennent de situations simples du quotidien : un email envoyé au mauvais destinataire, une pièce jointe non protégée, un mot de passe partagé, un document laissé sur une imprimante ou un fichier accessible à trop de personnes.

La sécurité n'est pas seulement l'affaire du service informatique. **Chaque professionnel a un rôle à jouer.**

## Exemples concrets

Un email envoyé avec tous les destinataires en copie visible.  
L'utilisation d'un mot de passe partagé entre plusieurs personnes.  
Un dossier papier laissé sans surveillance, accessible à des personnes non autorisées.



## Point d'attention

*Ne créez pas seul un compte sur un outil externe pour y stocker ou partager des données sensibles (usagers, patients, accompagnements). En cas de doute, demandez l'avis du DPO ou du service informatique avant utilisation.*

## Les bons réflexes



### Utiliser des mots de passe robustes

Un mot de passe doit être difficile à deviner, individuel et non partagé. Lorsque c'est possible, l'authentification à double facteur doit être activée.

### Verrouiller sa session

Dès que vous quittez votre poste, même pour quelques minutes, verrouillez votre session afin d'éviter toute consultation non autorisée.

### Limitier les accès

Chaque personne doit accéder uniquement aux données nécessaires à ses missions.

### Être vigilant avec les emails

Avant tout envoi, vérifiez les destinataires, les personnes en copie, la pièce jointe et le niveau de sensibilité des informations transmises.

### Faire valider les outils externes

Les outils en ligne (cloud, espaces collaboratifs ou solutions de transfert) doivent être vérifiés avant usage.

### Protéger aussi le papier et les supports mobiles

Les dossiers papier, ordinateurs portables, téléphones, clés USB et disques externes doivent être rangés, protégés et détruits ou restitués selon les règles internes.

# VII. Respecter les droits des personnes

Les personnes concernées disposent de **droits sur leurs données**. Ces droits leur permettent de **comprendre, vérifier, corriger** ou **demandeur certaines actions sur leurs informations**. Une demande peut arriver de différentes façons : par **email, courrier, formulaire, téléphone** ou **lors d'un échange**. Elle peut être très simple, par exemple : « je veux accéder à mon dossier », « je veux corriger mon adresse », « je ne veux plus recevoir de messages » ou « supprimez mes données ».

## Bon réflexe



- Ne pas ignorer la demande
- Noter la date de réception
- Transmettre rapidement la demande au DPO ou au relais RGPD
- Éviter de répondre seul à une demande complexe
- Conserver les éléments utiles et vérifier l'identité lorsque cela est nécessaire.

Le délai de réponse est en principe d'un mois à compter de la réception de la demande. Il est donc important d'alerter rapidement le DPO ou le relais RGPD.

## Réflexe DPO

Transmettez au DPO ou au relais RGPD toute demande portant sur un dossier, une modification, une suppression, un refus de transmission ou un accès aux données.

Toutes les demandes ne se traitent pas de la même façon : certaines nécessitent une analyse du contexte, de la base légale et des obligations de conservation. En cas de doute, il vaut mieux transmettre que répondre seul.

## Repère - Les principaux droits

- **Le droit d'accès** : une personne peut demander si la structure détient des données la concernant et en obtenir une copie. *Exemple : un usager demande à consulter son dossier.*
- **Le droit de rectification** : une personne peut demander la correction d'une information inexacte ou incomplète. *Exemple : une personne signale une erreur dans son adresse, ou ses coordonnées.*
- **Le droit d'effacement** : une personne peut demander la suppression de certaines données. Ce droit peut être limité selon les obligations légales de conservation.
- **Le droit d'opposition** : une personne peut refuser l'utilisation des données, selon leur base légale et le contexte.
- **Le droit à la limitation** : Une personne peut demander la suspension temporaire de l'utilisation de ses données.
- **Le droit à la portabilité** : dans certains cas, une personne peut récupérer ses données dans un format utilisable ou demander leur transmission à un autre organisme.

# VIII. Réagir en cas d'incident de sécurité

Un incident de sécurité est une situation qui met en danger des données personnelles : erreur, perte, accès non autorisé ou attaque informatique.

Cela peut arriver facilement au quotidien. L'important est de réagir vite. L'objectif n'est pas de sanctionner, mais de comprendre, limiter les risques et protéger les personnes.

## Exemples concrets

- Email envoyé au mauvais destinataire
- Ordinateur, clé USB ou dossier papier perdu ou volé
- Accès donné à une personne non autorisée
- Fichier partagé trop largement
- Compte piraté ou mot de passe divulgué

## Bon réflexe



- Alerter rapidement le responsable, le relais RGPD et/ou le DPO afin d'évaluer la situation et les actions à mener
- Décrire ce qui s'est passé
- Identifier les données et les personnes concernées
- Conserver les éléments utiles (email, capture, fichier ou message d'erreur)
- Prendre les premières mesures simples

## Point d'attention



Certains incidents doivent être signalés à la CNIL dans un délai court. C'est pourquoi il est essentiel d'alerter immédiatement en interne.

## Ce qu'il ne faut pas faire

- Évitez d'attendre plusieurs jours,
- Supprimer les preuves,
- Répondre seul aux personnes concernées,
- Contacter une autorité sans coordination interne ou de minimiser l'incident.

Si un outil semble compromis, son utilisation doit être vérifiée avec les personnes compétentes avant de continuer.

## Bon réflexe



En cas de doute, signalez. Un incident signalé rapidement est souvent maîtrisé.

# Conclusion

Passer des bons réflexes  
à une conformité accompagnée

**Ce guide permet de poser les bases :** comprendre ce qu'est une donnée personnelle, identifier les principaux usages, repérer les situations sensibles, adopter les premiers réflexes de sécurité, reconnaître une demande d'exercice de droits ou un incident.

Ces réflexes sont essentiels. Toutefois, ils ne suffisent pas à garantir une conformité RGPD complète et durable.

La conformité ne se limite pas à des principes. Elle s'applique à des situations concrètes, avec des choix à faire, des outils à encadrer, des pratiques à sécuriser et un suivi dans le temps.

Le guide permet de comprendre les bases, mais ne remplace pas l'analyse des situations concrètes.

**L'appui du DPO mutualisé peut vous permettre de passer des bons réflexes à une démarche plus structurée et sécurisée.** Il aide à adapter le RGPD aux pratiques réelles, à prioriser les actions et à sécuriser les situations sensibles.

#### **Il peut intervenir notamment pour :**

- Organiser les traitements et le registre
- Accompagner les demandes des personnes et les incidents
- Vérifier les outils et les partages de données
- Apporter un regard extérieur sur les pratiques.

L'objectif est de simplifier la mise en conformité et d'apporter de la sécurité au quotidien.

## **Pourquoi faire appel au DPO mutualisé ?**

Faire appel à un DPO mutualisé, c'est bénéficier d'un appui méthodologique et d'une expertise, sans avoir à gérer seul des questions parfois complexes.

### **Pour quels bénéfices ?**

- Gagner du temps dans la compréhension des obligations
- Avancer de façon progressive et adaptée
- Éviter les erreurs d'interprétation
- Prioriser les actions réellement utiles
- Sécuriser les pratiques sensibles
- Disposer de la documentation adéquate pour démontrer la conformité

### **Quand le solliciter ?**

L'appui du DPO est particulièrement utile en cas de :

- Traitement de données sensibles (santé, social...)
- Mise en place ou évolution d'un outil
- Partage de données avec des partenaires
- Demande d'exercice de droits
- Incident ou doute sur une situation

## **Message clé**

En matière de données personnelles, mieux vaut poser une question en amont que gérer un problème ensuite.

Le bon réflexe n'est pas de tout gérer seul, mais de savoir quand mobiliser un appui pour sécuriser ses pratiques et accompagner la conformité dans la durée.



## Repère - Les ressources utiles pour aller plus loin

Pour approfondir ou vérifier certaines pratiques ou sensibiliser vos équipes, plusieurs ressources peuvent vous être utiles :

**Ces ressources peuvent vous aider à compléter votre compréhension, mais ne remplacent pas l'analyse adaptée à votre situation.**

**CNIL – Guides pratiques RGPD :** [www.cnil.fr](http://www.cnil.fr)

des ressources pour comprendre les obligations et répondre aux principales questions liées à la protection des données

**ANSSI – guides et recommandations :**

des ressources pour renforcer les bonnes pratiques en matière de cybersécurité

**CNIL – MOOC Atelier RGPD :**

une formation générale en ligne gratuite pour approfondir les fondamentaux du RGPD

**DPO mutualisé :**

un interlocuteur à solliciter pour toute situation spécifique, question ou doute sur une pratique.



## Et pour sensibiliser vos équipes ?

La conformité au RGPD ne repose pas uniquement sur la mise en place de procédures et d'outils. Elle repose aussi sur la compréhension et l'implication de l'ensemble des collaborateurs, qui sont au quotidien les premiers acteurs de la protection des données.

Une sensibilisation ponctuelle ne suffit pas : les pratiques, les outils et les risques évoluent. Il est donc important de sensibiliser régulièrement les équipes, de rappeler les bons réflexes et de maintenir une culture commune de la protection des données.

Quelques exemples de bonnes pratiques peuvent être régulièrement rappelés : vérifier les destinataires avant un envoi, protéger ses mots de passe, être vigilant face aux

messages suspects, respecter les règles de confidentialité ou encore utiliser les outils mis à disposition par la structure.

La sensibilisation peut prendre différentes formes : réunions d'équipe, ateliers, quiz, affiches, rappels thématiques, formations ou mises en situation. L'objectif est de faire de la protection des données un réflexe professionnel au quotidien.

***Pour en savoir plus sur l'offre d'accompagnement et les ressources proposées,***

**contactez :** [k.gordien@facs-occitanie.fr](mailto:k.gordien@facs-occitanie.fr)

## Repère - Les ressources utiles pour aller plus loin

Pour renforcer l'accompagnement des adhérents, la Fédération lancera en **janvier 2027** une nouvelle **plateforme de sensibilisation** dédiée à la **protection des données et à la cybersécurité**.



**Appui Santé Occitanie Services**

### Le RGPD et la cybersécurité, appris par la pratique.

Des parcours courts, des exercices dans chaque chapitre, des jeux d'évasion — et une attestation à la clé.

- Des parcours, du socle à l'expertise**  
RGPD, cybersécurité, formation métier.  
Et dix modules courts pour approfondir un sujet précis.
- Deux escape games**  
Une attaque à contenir, une demande de droits à traiter.  
Trente-cinq minutes, huit salles.
- Une évaluation et une attestation**  
Votre niveau est mesuré, votre attestation vous suit.

[parcours-rgpd.com](https://parcours-rgpd.com)

La plateforme sera accessible aux adhérents ayant souscrit à l'offre d'accompagnement. Elle permettra aux professionnels de se sensibiliser à leur rythme, grâce à des contenus pédagogiques variés et des activités interactives.

**Des formats ludiques**, notamment des escape-games, permettront d'aborder concrètement les principaux enjeux de la protection des données et de la cybersécurité et de développer les bons réflexes au quotidien.

La plateforme pourra être utilisée ponctuellement pour **approfondir un thème ou dans le cadre d'un parcours de sensibilisation**, permettant aux équipes de progresser étape par étape.

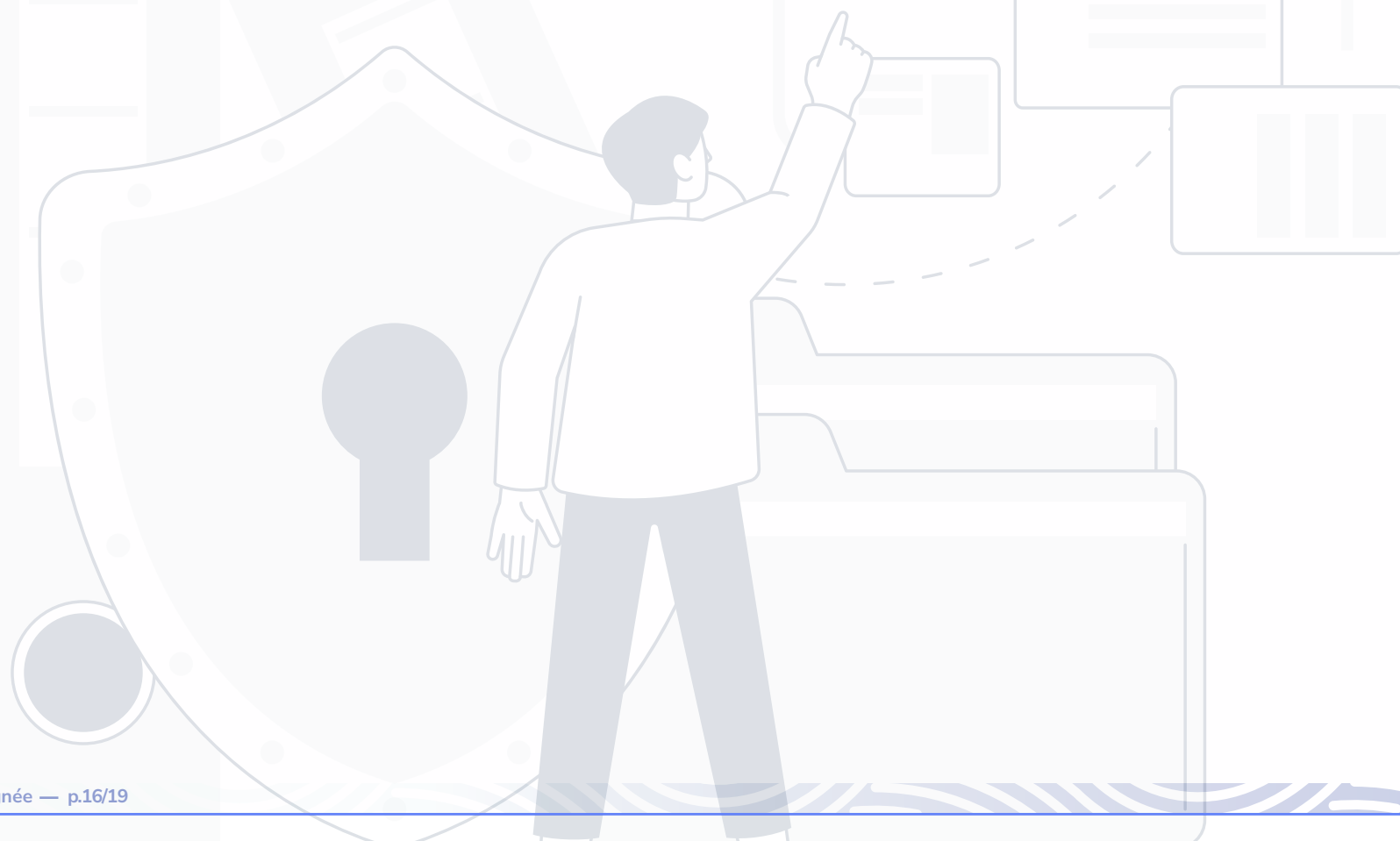
Elle viendra ainsi **compléter les actions de sensibilisation et les ressources proposées** dans le cadre de l'offre d'accompagnement du DPO mutualisé.

*Rendez-vous en janvier 2027 pour découvrir cette nouvelle ressource et accompagner vos équipes dans la durée.*

# Annexe — Auto-diagnostic

## Où en êtes-vous dans vos pratiques ?

Cet auto-diagnostic n'est pas un audit complet. Il permet d'identifier rapidement vos points forts et vos axes d'amélioration.



Pour chaque question, répondez par : Oui / Non / À vérifier.

## Compréhension des données

### Question

- Savons-nous identifier les données personnelles utilisées dans notre activité ?
- Savons-nous repérer les données sensibles (santé ou données sociales) ?
- Évitions-nous de collecter des informations inutiles ?
- Les informations saisies sont-elles utiles, objectives et proportionnées ?

| OUI | NON | À VÉRIFIER |
|-----|-----|------------|
|-----|-----|------------|

|  |  |  |
|--|--|--|
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Organisation des traitements

### Question

- Avons-nous identifié les principaux fichiers, logiciels et dossiers contenant des données ?
- Savons-nous à quoi sert chaque fichier ou outil ?
- Les accès aux données sont-ils clairement définis ?
- Les durées de conservation sont-elles connues et respectées ?

| OUI | NON | À VÉRIFIER |
|-----|-----|------------|
|-----|-----|------------|

|  |  |  |
|--|--|--|
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Sécurité

### Question

- Les mots de passe sont-ils individuels et robustes ?
- Les sessions sont-elles verrouillées en cas d'absence ?
- Les dossiers papier sont-ils sécurisés ?
- Les pièces jointes sensibles sont-elles envoyées avec prudence ?
- Les accès aux dossiers partagés sont-ils limités aux personnes concernées ?
- Les outils externes sont-ils validés avant utilisation ?

| OUI | NON | À VÉRIFIER |
|-----|-----|------------|
|-----|-----|------------|

|  |  |  |
|--|--|--|
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Droits des personnes et incidents

### Question

- Savons-nous reconnaître une demande liée aux droits des personnes ?  
Savons-nous à qui transmettre une demande d'accès, de rectification ou de suppression ?  
Savons-nous reconnaître un incident de sécurité ?  
Les équipes savent-elles qu'un incident doit être signalé rapidement ?  
Les incidents sont-ils remontés systématiquement ?

| OUI | NON | À VÉRIFIER |
|-----|-----|------------|
|     |     |            |
|     |     |            |
|     |     |            |
|     |     |            |
|     |     |            |

## Interpréter les réponses

- Si la majorité des réponses sont **OUI**, les premiers réflexes sont installés. Il reste utile de les maintenir et de les vérifier régulièrement.
- Si plusieurs réponses sont **À VÉRIFIER**, un échange avec le DPO peut aider à clarifier les pratiques.
- Si plusieurs réponses sont **NON**, il est recommandé de prioriser un plan d'action simple : accès, sécurité, inventaire, information des personnes, gestion des incidents.

### Bon réflexe

L'auto-diagnostic peut être utilisé en équipe pour identifier quelques actions simples à mettre en œuvre rapidement avec l'appui du DPO mutualisé si besoin.



# Annexe

## Mini-fiche réflexe

### À afficher ou diffuser

#### Avant de collecter une donnée

- Posez-vous une question simple : est-ce vraiment nécessaire ?
- La personne comprend-elle pourquoi vous la demandez ?
- En cas de doute, demandez conseil.

#### Avant d'envoyer un email

- Vérifiez les destinataires, les pièces jointes et le contenu.
- Attention aux données sensibles ou aux envois en nombre.

#### Avant de créer un fichier

- Existe-t-il déjà un outil ?
- Qui y aura accès ?
- Où sera-t-il stocké ?
- Combien de temps sera-t-il conservé ?

#### En cas de demande d'une personne

- Notez la demande et la date.
- Transmettez-la rapidement au relais RGPD ou au DPO.
- Évitez de répondre seul si vous avez un doute.

#### En cas d'incident

- Décrivez les faits.
- Conservez les éléments utiles.
- Suivez les consignes du relais RGPD ou du DPO.