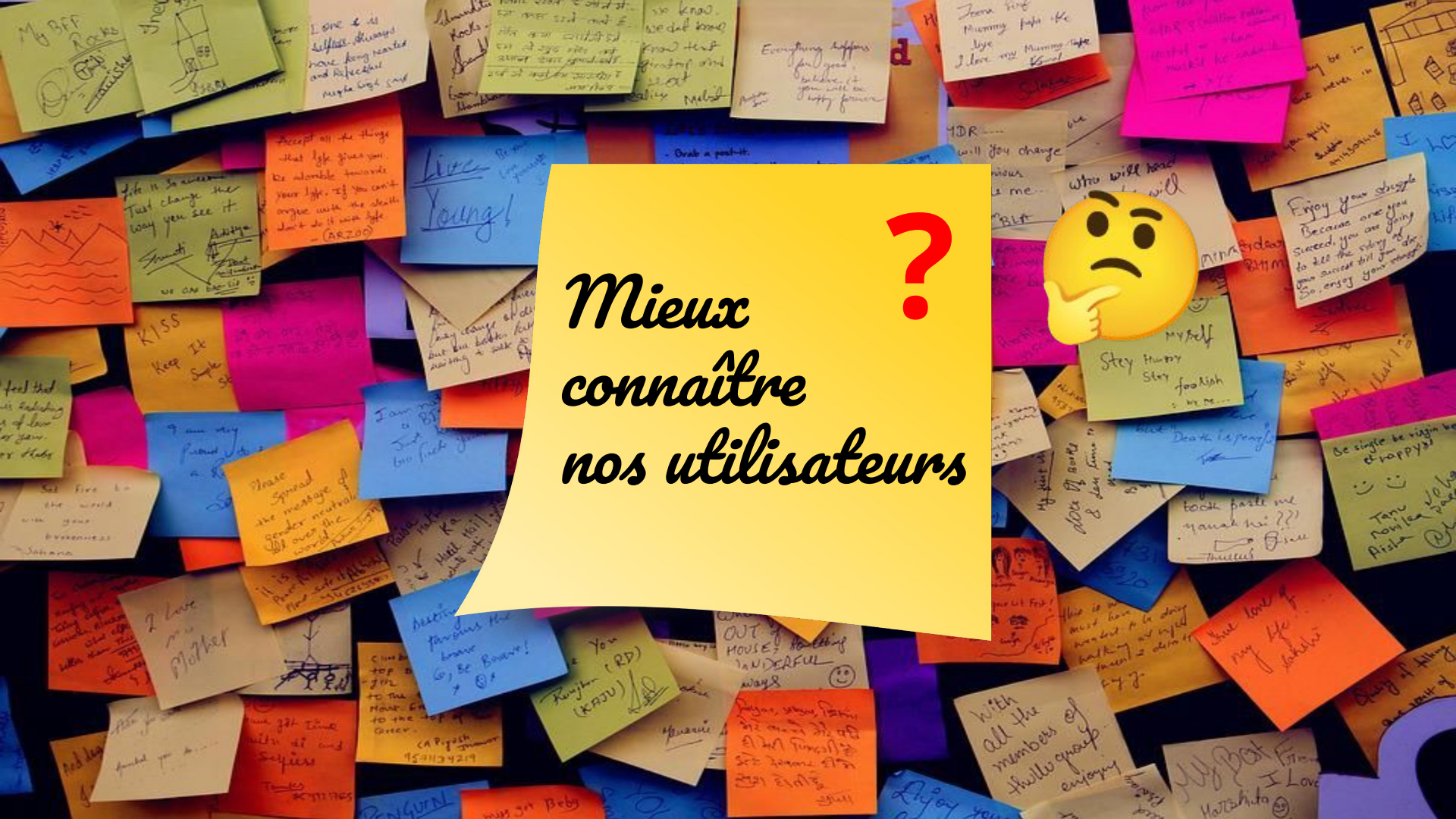

Devfest
LILLE 22


Mieux connaître nos utilisateurs
?

Quelques heures plus tard...


Êtes-vous conformes au RGPD ?

$ whoami

François DELBRAYELLE (@fdelbrayelle)

Cht'Ippon chez **Ippon** Lille depuis 2019

- ***Senior Software Engineer***
- ***Tech Community Ambassador***
- **Formateur**
- Référent blog.ippon.fr

Contributeur OSS / **JHipster**


ippon
27/9/21
LILLE
CHALEUREUX!
MARQUES
DEV FULL-STACK
TRANSFORMATION
DEVOPS CLOUD
ENTRAIDE
PROGRESSER
MISSIONS STIMULANTES
RESPONSABILITÉS
HUMAIN
CHALLENGES
CO-CONSTRUCTION
COLLECTIVE ENERGY
ARTHUR, T'AS GAGNÉ!
VAN STRATEGY OFFICER
...OU PAS...
ON FOUT DES BAFFES!
ACCOMPAGNEMENT
CHIEF OF BEERS
CHIEF STRATEGY OFFICER
MODERN ARCHITECT
DELIVERY AVOCAT
GOODIES' DIRECTOR
ON EST TOUS LEADERS!
BIENVEILLANCE
GÉNÉREUX
25 PERSONNES!
AVRIL 2019
TOP ambiance!
ADEO
VEOLIA
LEROY MERLIN
CRAFT
GALERIES LAFAYETTE
EDF
NEXITY
CONTRIBUTION
ACCUEIL STAGIAIRES
FORMATION
SITE WEB
MEETUP
DEVFEST
COMMUNAUTÉS
CLOUD NORD
PARTAGE DE CONNAISSANCES
JAVA
DESIGN
POSITIVE TECHNOLOGY
TIENT SES PROMESSES
TECH' SYMPA!
SCALE ACCÉLÉRALE INNOVALE!
2024
QUALITY FIRST!
AURA DANS L'IT
POURQUOI?
VOILÀ COMMENT...
OLIVIER SAMPSON-
Devfest LILLE 22


Devfest
LILLE 22
RGPD pour
les développeurs

SAFARI (1974)

Système automatisé pour les fichiers administratifs et le répertoire des individus

REJECTED

Loi Informatique et Libertés (1978)

Représentation de la donnée

1 char (ex : ‘a’) = 1 octet = 8 bits

1 Ko = 1 000 octets

1 Mo = 1 000 000 octets

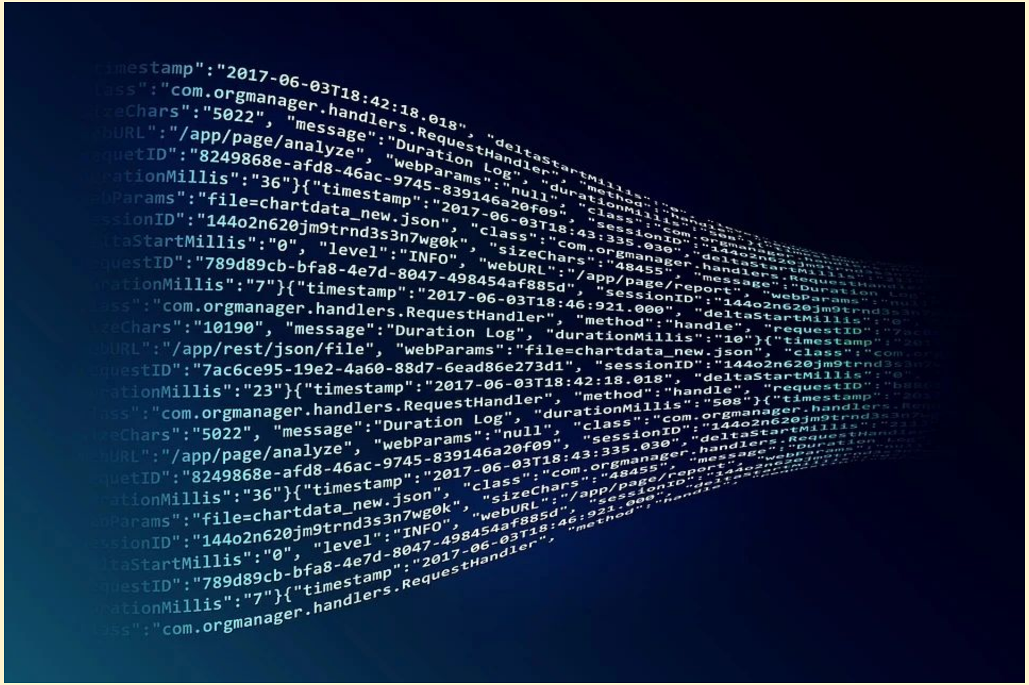
1 Go = 1 000 000 000 octets

1 To = 1 000 000 000 000 octets => mille milliards de ‘a’ 💥

1 Po = 1 000 000 000 000 000 octets

1 Eo = 1 000 000 000 000 000 000 octets

Data is the new gold 🪙



Règlement Général sur la Protection des Données

🇪🇺 **Règlement UE 2016/679** du Parlement européen et du Conseil du 27 avril 2016

173 considérants, 99 articles

Entré en vigueur le 25 mai 2018

Inspiré par la loi Informatique et Libertés de 1978

En anglais : *General Data Protection Regulation* (GDPR)

🛠 Outils du RGPD

DPO

Registre des activités de traitement

Analyse d'impacts sur la vie privée (PIA)

🛠 Outils du RGPD

DPO

Registre des activités de traitement

Analyse d'impacts sur la vie privée (PIA)

🛠 Outils du RGPD

DPO

Registre des activités de traitement

Analyse d'impacts sur la vie privée (PIA)

🛠 Outils du RGPD

DPO

Registre des activités de traitement

Analyse d'impacts sur la vie privée (PIA)

👨 Acteurs en jeu

Personne concernée

Responsable de traitement

Sous-traitant

👨‍💼 Acteurs en jeu

Personne concernée

Responsable de traitement

Sous-traitant

👨 Acteurs en jeu

Personne concernée

Responsable de traitement

Sous-traitant

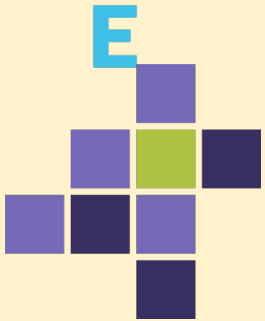
👨‍💼 Acteurs en jeu

Personne concernée

Responsable de traitement

Sous-traitant

👮 Qui contrôle ?



- https://www.cnil.fr/fr/guide-rgpd-du-developpeur
- https://github.com/LINCnil/Guide-RGPD-du-developpeur/

📝 Fiche n°0 : Développer en conformité avec le RGPD

⚠️ **(Se) sensibiliser** aux grands principes du RGPD

💡 **Cartographier** et catégoriser **les données et les traitements** de votre système

💡 Organiser des processus internes pour la **conformité** durant toutes les étapes

💡 Créer un **dépôt git** pour versionner **cette documentation**

💡 Se reposer sur son **DPO**

📝 Fiche n°1 : Identifier les données à caractère personnel

⚠️ Tout ce qui **identifie** une personne

⚠️ **Traitements** licites (toute opération sur ces données)
avec **finalités** précises et déterminées *a priori*

Qu’est-ce qu’un traitement ?

« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que ***la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction*** *»*

RGPD - Chapitre I - Article 4 - Définitions

Cas de l'intelligence artificielle

« La personne concernée a le droit ***de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé*** *[…] produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. »*

RGPD - Chapitre III - Article 22 - Droits de la personne concernée

📝 Fiche n°1 : Identifier les données à caractère personnel

⚠️ Tout ce qui **identifie** une personne

⚠️ **Traitements** licites (toute opération sur ces données)
avec **finalités** précises et déterminées *a priori*

💡 **Anonymisation ou pseudonymisation**

⚠️ **Utilisation frauduleuse** personnelle ou professionnelle

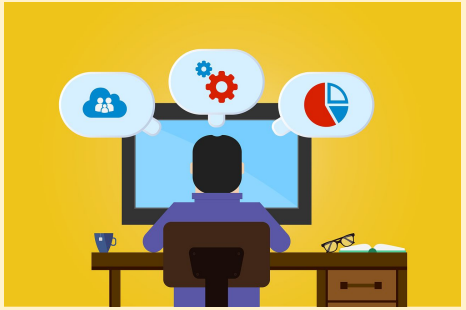
🚩 **Démo conforme ?**

📝 Fiche n°2 : Préparer son développement

💡 ***Privacy by design* et *privacy by default***

💡 **Normes de développement**

⚠️ **Langages ou technos utilisés**



📝 Fiche n°3 : Sécuriser ses environnements

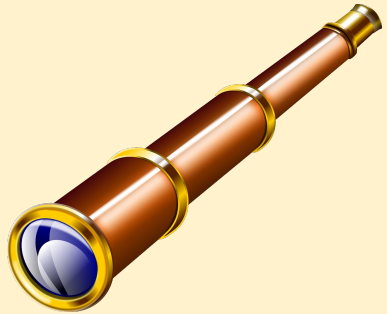
- 💡 **Sécurisation homogène**
- 💡 **Outils d'automatisation** (Terraform, Ansible, Chef…)
- ⚠️ **Risques liés aux outils SaaS** (*Software as a Service*)
- 💡 **Durée de vie limitée des *tokens***

📝 Fiche n°4 : Gérer son code source

- 💡 ***Source Control Management***
- 💡 **Stratégie de *branching***
- 💡 **Revue de code minutieuse**
- ⚠️ **Secrets protégés** (HashiCorp Vault)

📝 Fiche n°5 : Faire un choix éclairé de son architecture

- 💡 **Cycle de vie** des données personnelles
- 💡 Choix des **supports de stockage**
- 💡 ***On premise*** ou ***cloud*** **?**
- ⚠️ **Localisation géographique**
- 💡 **Certification HDS* pour les données de santé** (sensibles)



* hébergeur de données de santé

📝 Fiche n°6 : Sécuriser les sites web et applications

- 💡 **Sécuriser les bases de données** (données stockées)
- 💡 **Sécuriser les communications** (données transférées)
- 💡 **Sécuriser les authentifications**
- 💡 **Sécuriser les infrastructures**
- 💡 **Veille vulnérabilités (bulletin CERT : https://www.cert.ssi.gouv.fr)**
- ⚠️ **Ne pas divulguer d'informations dans les erreurs**

📝 Fiche n°7 : Minimiser les données collectées

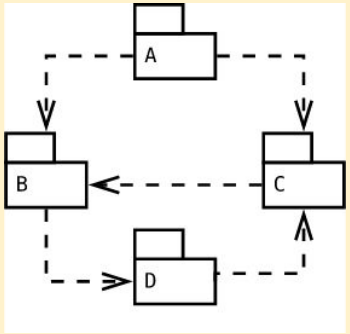
- 💡 Restreindre la collecte au **strict nécessaire** (YAGNI)
- 💡 **Réduire leur précision**
- ⚠️ **Champs libres**
- ⚠️ **Logs** (6 mois à 1 an)
- 💡 **Purge des données**
- 🚩 **Démo conforme ?**

📝 Fiche n°8 : Gérer les utilisateurs

- 💡 **Identifiants uniques**
- 💡 **Authentification forte**
- 💡 **Principe du moindre privilège**
- 💡 **Tracer les activités**
- ⚠️ **Limiter les super pouvoirs**

📝 Fiche n°9 : Maîtriser les dépendances

- 💡 **Intérêt d'une dépendance**
- ⚠️ **Dépendances maintenues** (fin de vie ?)
- 💡 **Documentation**
- ⚠️ **Transfert hors UE encadré**
- 💡 **Contrat de sous-traitance**
- 💡 **Rapports d'audit et gestion des dépendances**
- 🚩 **Démo conforme ?**



📝 Fiche n°10 : Qualité du code et documentation

- 💡 Contrôler la **qualité du code**
- 💡 Contrôler la **sécurité du code**
- 💡 Adopter des **conventions de nommage**
- 💡 **Documenter le code et l'architecture**
- ⚠️ ***Developer experience*** **(DevX)**

📝 Fiche n°11 : Tester vos applications

- 💡 **Automatiser**
- 💡 **Tests de sécurité**
- 💡 ***Chaos engineering*** (Istio, Netflix Simian Army…)
- ⚠️ **Aucune donnée personnelle dans les tests**

📝 Fiche n°12 : Informer les personnes

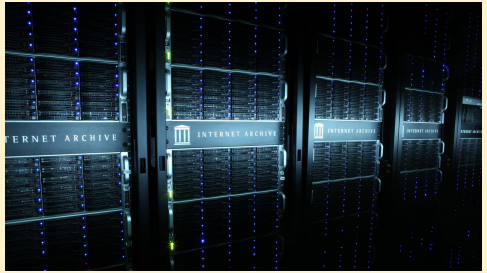
- 💡 **Pleine conscience**
- 💡 **Collecte directe ou indirecte**
- 💡 **Informations sur l'organisme collecteur**
- 💡 **Forme variable**
- ⚠️ **Signaler les incidents**

📝 Fiche n°13 : Préparer l'exercice des droits des personnes

- 💡 Droits d'**information**, d'**accès**, de **rectification**, d'**opposition**, d'**effacement**
- 💡 Nouveaux droits à l'**oubli**, à la **portabilité**, au **non profilage** et à la **limitation**
- 💡 **Accessibilité**
- 💡 **Garder une trace** (base de données, *event sourcing*)
- ⚠️ Délai standard de traitement d'une requête relative à un droit : **30 jours**
- ⚠️ **8 jours pour les données de santé**

📝 Fiche n°14 : Gérer la durée de conservation des données

- 💡 **Base active**
- 💡 **Archivage intermédiaire**
- 💡 **Archivage définitif ou purge**



📝 Fiche n°15 : Les bases légales dans l'implémentation

💡 **Justification du traitement**

💡 **Contrat, intérêt légitime ou consentement**

💡 **Obligation légale ou mission d'intérêt public**

⚠️ **1 traitement = 1 à n finalités ; 1 finalité = 1 seule base légale**

⚠️ **Données sensibles :**
exception prévue en complément par l'article 9 du RGPD

Données personnelles	Finalités	Bases légales
Civilité /Nom / prénom	- Fournir le produit ou le service à la personne nommément éligible (ex: programme de fidélité, conseiller de vente personnalisé, commande, service de cagnotte). - Améliorer nos services et votre expérience client - Personnaliser nos communications - Établir un document nominatif : une facture ou une garantie… - Participation à un jeu concours - Réaliser des analyses statistiques	- Exécuter un contrat - Intérêt légitime, améliorer nos services
Adresse postale	- Vous identifier - Expédier et livrer vos commandes - Établir un document nominatif : une facture ou une garantie… - Vous contacter et vous adresser des documents vous concernant - Gérer votre participation à un jeu concours: envoi des dotations. - Le cas échéant, vérification du domicile par l'organisme de crédit ou par toute autorité administrative compétente (détaxe). - Réaliser des analyses statistiques	- Exécuter un contrat - Intérêt légitime, améliorer nos services - Obligation légale
Adresse e-mail	-- Vous identifier - Vous contacter - Vous informer - Vous inviter à des événements - Vous adresser des sollicitations commerciales si vous y avez consent	- Exécuter un contrat - Intérêt légitime, améliorer nos services - Consentement

📝 Fiche n°16 : Les traceurs

⚠️ **Consentement avant stockage ou accès**

🍪 **Cookies traceurs ou pixels espions**

⚠️ **Finalités avec consentement obligatoire**

🍪 **Traceurs exemptés de consentement**

💡 **Case à cocher ☐ ⇒ ☑️**

💡 **Stocker les preuves de consentement**

💡 **DevTools** (F12)

🚩 **Démo conforme ?**

📝 Fiche n°17 : Mesurer la fréquentation des applications

🍪 **Cookies traceurs**

💡 **Information des utilisateurs avec opposition possible**

⚠️ **Exemption de consentement envisageable**

⚠️ **Conversation maximum 25 mois**

📝 Fiche n°18 : Se protéger des attaques informatiques

💡 **Sécurité = confidentialité, intégrité, disponibilité, traçabilité**

⚠️ **Violation = destruction, perte, altération ou divulgation**

💡 **Top 10 OWASP + Webgoat**

OWASP

- https://www.cnil.fr/fr/guide-rgpd-du-developpeur
- https://github.com/LINCnil/Guide-RGPD-du-developpeur/

En résumé

🏫 **(Se) sensibiliser** en tant que développeur ou non développeur

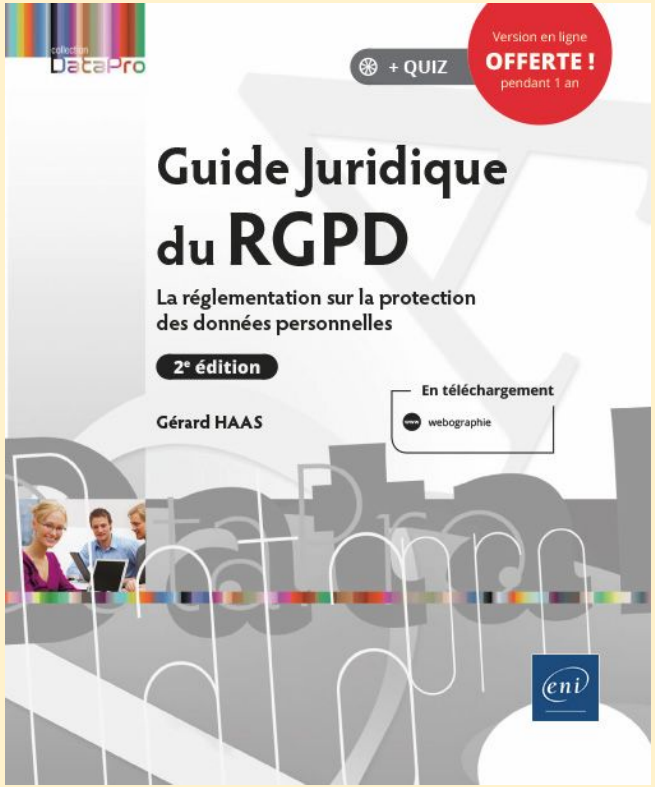
💡 Avoir les **bons réflexes sur les données personnelles**

🔒 Appliquer les **mesures de protection** et de **sécurité**

⚠️ **Alerter en cas d'incident**

🤝 Avoir un **devoir de conseil technique** auprès de ses clients

🧐 Faire de la **veille** pour s'informer (sécurité, RGPD...)


collection DataPro
+ QUIZ
Version en ligne
OFFERTE !
pendant 1 an
Guide Juridique du RGPD
La réglementation sur la protection des données personnelles
2e édition
Gérard HAAS
En téléchargement
webographie
eni


collection DataPro
Version en ligne
OFFERTE !
pendant 1 an
RGPD
Le comprendre et le mettre en œuvre
(retours d'expérience pour les DPO, responsables d'entreprise, responsables informatique, chefs de projet...)
Jacques FOUCAULT
Loïc PANHALEUX
Dominique RENAUD
Pierre BEGASSE
2e édition
eni

ippon

Merci ! 🙏

Avez-vous des questions ?

www.ippon.fr

contact@ippon.fr —— +33 1 46 12 48 48 —— @ipponTech