BLOC 3

TRAITER

Le RGPD et la protection des données

1h30

Mon application collecte des données personnelles, que dois-je faire ?

Objectifs du Bloc 3

À l'issue de ce bloc, vous saurez :

- Identifier ce qu'est une donnée personnelle (et ce qui n'en est pas)
- Connaître les 6 bases légales qui autorisent un traitement
- Comprendre les droits des personnes sur leurs données
- Appliquer les obligations essentielles du développeur
- Formaliser les règles RGPD avec la méthode algébrique

RGPD = Règlement Général sur la Protection des Données

En vigueur depuis le 25 mai 2018 - Applicable dans toute l'Union Européenne

Pourquoi le RGPD existe-t-il ?

Contexte : l'explosion des données numériques

- Réseaux sociaux, e-commerce, applications mobiles...
- Collecte massive de données sur les individus
- Scandales (Cambridge Analytica, fuites de données...)
- Besoin d'un cadre juridique unifié en Europe

Objectifs du RGPD :

Protéger	Responsabiliser	Harmoniser
Les droits fondamentaux des personnes sur leurs données	Les entreprises qui collectent et traitent les données	Les règles dans tous les pays de l'UE

Sanctions possibles : jusqu'à 20 millions € ou 4% du CA mondial

Qu'est-ce qu'une donnée personnelle ?

Article 4 du RGPD - Définition :

"Toute information se rapportant à une personne physique identifiée ou identifiable [...] directement ou indirectement, notamment par référence à un identifiant"

Deux conditions cumulatives :

1. C'est une INFORMATION	ET	2. Elle IDENTIFIE une personne
Texte, nombre, image, son, localisation, comportement...		Directement (nom) ou indirectement (croisement)

```
EST_DONNEE_PERSONNELLE = EST_INFORMATION AND (IDENTIFIEE OR IDENTIFIABLE)
```

Attention : une personne "identifiable" suffit (pas besoin d'être déjà identifiée)

Exemples : donnée personnelle ou non ?

DONNÉES PERSONNELLES

- Nom, prénom
- Adresse email
- Numéro de téléphone
- Adresse IP
- Identifiant de cookie
- Photo du visage
- Données de géolocalisation
- Numéro de sécurité sociale
- Plaque d'immatriculation
- Empreinte digitale

NON PERSONNELLES

- Numéro SIRET (entreprise)
- Données anonymisées*
- Statistiques agrégées
- Données sur personnes morales
- Informations génériques
  (ex: "un habitant de Paris")

* Attention : pseudonymisées ≠ anonymisées

Attention aux données "indirectement" identifiantes !

Exemple : Âge + Code postal + Profession = identification possible dans 87% des cas (étude MIT)

Les données sensibles (catégories particulières)

Article 9 du RGPD : certaines données sont INTERDITES de traitement par défaut

Catégories de données sensibles :

- Origine raciale ou ethnique
- Opinions politiques
- Convictions religieuses ou philosophiques
- Appartenance syndicale
- Données génétiques
- Données biométriques (identification)
- Données de santé
- Vie sexuelle ou orientation sexuelle

```
TRAITEMENT_SENSIBLE_AUTORISE =
    EST_DONNEE_SENSIBLE AND
    (CONSENTEMENT_EXPLICITE OR EXCEPTION_LEGALE)
```

Exceptions principales : consentement explicite, obligations légales, intérêt vital, médecine du travail...

Pour le développeur : une appli fitness collectant le rythme cardiaque traite des données de SANTÉ !

Qu'est-ce qu'un "traitement" de données ?

Article 4 du RGPD - Définition très large :

"Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel"

Exemples de traitements :

Collecte :	Formulaire d'inscription	**Consultation :**	Affichage d'un profil utilisateur
Enregistrement :	Stockage en base de données	**Utilisation :**	Envoi d'emails marketing
Organisation :	Classement par catégorie	**Transmission :**	Partage avec un prestataire
Conservation :	Archivage des données	**Effacement :**	Suppression d'un compte

En pratique : dès que votre code manipule des données personnelles,
vous effectuez un traitement soumis au RGPD

Les 6 bases légales du traitement

Article 6 du RGPD : tout traitement DOIT reposer sur une base légale

```
TRAITEMENT_LICITE = BASE_LEGALE_VALIDE AND FINALITE_DETERMINEE AND DONNEES_ADEQUATES
```

Les 6 bases légales possibles :

1. Consentement

La personne a donné son accord

2. Contrat

Nécessaire à l'exécution d'un contrat

3. Obligation légale

Imposé par la loi

4. Intérêts vitaux

Protection de la vie

5. Mission publique

Service public

6. Intérêt légitime

Intérêt de l'organisme (équilibré)

En pratique pour un développeur : principalement consentement, contrat et intérêt légitime

Base légale n°1 : Le consentement

La base légale la plus connue... et la plus exigeante

Le consentement doit être :

L	**Libre**	Sans contrainte ni conséquence négative en cas de refus
S	**Spécifique**	Pour chaque finalité distincte
E	**Éclairé**	Après information claire et complète
U	**Univoque**	Par un acte positif clair (pas de case pré-cochée)

```
CONSENTEMENT_VALIDE = LIBRE AND SPECIFIQUE AND ECLAIRE AND UNIVOQUE
```

+ Le consentement doit pouvoir être retiré à tout moment, aussi facilement qu'il a été donné

Consentement : bonnes et mauvaises pratiques

INVALIDE

✗ Case pré-cochée
✗ "En continuant, vous acceptez..."
✗ Consentement groupé pour plusieurs finalités
✗ Refus = pas d'accès au service
✗ Bouton "Refuser" caché ou compliqué

VALIDE

✓ Case à cocher (non pré-cochée)
✓ Information claire avant validation
✓ Une case par finalité
✓ Service accessible même sans consentement
✓ Boutons "Accepter" et "Refuser" équivalents

Exemple : Bannière de cookies

❌ Non conforme

"Ce site utilise des cookies.
[Accepter tout]"
(pas de bouton refuser)

✓ Conforme

"Ce site utilise des cookies pour...
[Personnaliser] [Tout refuser] [Tout accepter]"

Base légale n°6 : L'intérêt légitime

Alternative au consentement quand celui-ci n'est pas adapté

Conditions d'utilisation :

- L'intérêt poursuivi est légitime (pas illégal, pas contraire à l'éthique)
- Le traitement est nécessaire (pas d'autre moyen moins intrusif)
- Les droits des personnes ne prévalent PAS sur cet intérêt

```
INTERET_LEGITIME_VALIDE =
    INTERET_LEGITIME AND
    TRAITEMENT_NECESSAIRE AND
    NOT(DROITS_PERSONNE_PREVALENT)
```

Exemples d'utilisation :

- Sécurité du réseau (logs de connexion)
- Prévention de la fraude
- Marketing direct auprès de clients existants (avec opt-out facile)
- Amélioration des services (analytics limités)

Base légale n°2 : L'exécution d'un contrat

Utilisable quand le traitement est nécessaire pour exécuter un contrat

Conditions :

- Un contrat existe entre vous et la personne concernée
- Le traitement est NÉCESSAIRE à l'exécution de ce contrat
- La personne est partie au contrat

BASE CONTRAT OK

- Adresse de livraison pour e-commerce
- Email pour confirmation de commande
- Coordonnées bancaires pour paiement
- Données pour créer un compte client

BASE CONTRAT NON

- Publicité ciblée (pas nécessaire)
- Partage avec partenaires marketing
- Profilage comportemental
- Newsletter (sauf si dans le contrat)

```
BASE_CONTRAT_VALIDE = CONTRAT_EXISTE AND PERSONNE_PARTIE_AU_CONTRAT AND TRAITEMENT_NECESSAIRE_EXECUTION
```

Les droits des personnes concernées

Le RGPD confère des droits aux personnes dont vous traitez les données

Droit d'accès

Obtenir confirmation et copie des données

Droit de rectification

Corriger les données inexactes

Droit à l'effacement

"Droit à l'oubli" - suppression des données

Droit à la limitation

Geler temporairement le traitement

Droit à la portabilité

Récupérer ses données dans un format réutilisable

Droit d'opposition

S'opposer au traitement (notamment marketing)

Délai de réponse : 1 mois maximum (prolongeable à 3 mois si complexe)

Pour le développeur : votre application DOIT permettre l'exercice de ces droits !

Zoom sur le droit d'accès (article 15)

La personne peut demander :

- Confirmation que ses données sont traitées (ou non)
- Copie de TOUTES les données personnelles détenues
- Informations sur : finalités, catégories, destinataires, durée de conservation
- Source des données (si pas collectées directement)
- Existence d'une décision automatisée (profilage)

Implémentation technique recommandée :

- Fonction d'export des données utilisateur (JSON, CSV)
- Page "Mes données" dans le profil utilisateur
- Formulaire de demande d'accès avec vérification d'identité
- Journalisation des demandes et réponses

Gratuit pour la personne (sauf demandes manifestement abusives)

Zoom sur le droit à l'effacement (article 17)

La personne peut demander la suppression de ses données si :

- Les données ne sont plus nécessaires aux finalités initiales
- Le consentement est retiré (et pas d'autre base légale)
- La personne s'oppose au traitement (et pas de motif légitime)
- Le traitement est illicite
- Obligation légale d'effacement

MAIS ce droit n'est PAS absolu - Exceptions :

- Liberté d'expression et d'information
- Obligation légale de conservation (factures, contrats...)
- Intérêt public (archives, recherche scientifique)
- Constatation ou défense de droits en justice

Implémentation : prévoir une fonction de suppression complète du compte et des données associées

```
DOIT_EFFACER = DEMANDE_EFFACEMENT AND (CAS_EFFACEMENT_VALIDE) AND NOT(EXCEPTION_APPLICABLE)
```

Zoom sur le droit à la portabilité (article 20)

La personne peut récupérer ses données dans un format réutilisable

Conditions d'application :

- Base légale = consentement OU contrat (pas intérêt légitime)
- Traitement automatisé (pas les dossiers papier)
- Données FOURNIES par la personne (pas les données dérivées)

Exigences techniques :

- Format structuré : JSON, XML, CSV
- Lisible par machine (pas de PDF image)
- Couramment utilisé (standards ouverts)
- Possibilité de transfert direct vers un autre service (si techniquement faisable)

Exemple : Export des données utilisateur en JSON avec toutes les informations fournies

```
{ "nom": "Dupont", "email": "dupont@email.com", "historique_achats": [...] }
```

Obligations du responsable de traitement

Le "responsable de traitement" est celui qui décide du POURQUOI et du COMMENT

Principales obligations :

Information	Informer les personnes sur le traitement (politique de confidentialité)
Sécurité	Protéger les données contre les violations (mesures techniques)
Minimisation	Ne collecter que les données strictement nécessaires
Limitation durée	Ne pas conserver les données plus longtemps que nécessaire
Accountability	Pouvoir démontrer sa conformité (documentation)
Privacy by design	Intégrer la protection des données dès la conception

Vous êtes développeur = vous êtes acteur de la conformité RGPD

Privacy by Design : le RGPD dans le code

Article 25 : Protection des données dès la conception et par défaut

7 principes du Privacy by Design :

1. Proactif, pas réactif (anticiper les risques)
2. Protection par défaut (paramètres les plus protecteurs)
3. Protection intégrée à la conception
4. Fonctionnalité complète (pas de compromis)
5. Sécurité de bout en bout
6. Transparence et visibilité
7. Respect de la vie privée de l'utilisateur

En pratique pour le développeur :

- Chiffrement des données sensibles en base
- Cases non pré-cochées par défaut
- Collecte minimale de données dès le formulaire
- Purge automatique des données périmées

Obligation de sécurité (article 32)

Mesures techniques et organisationnelles appropriées

Le RGPD cite notamment :

- Pseudonymisation et chiffrement des données
- Moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité
- Moyens de rétablir la disponibilité des données en cas d'incident
- Procédure pour tester et évaluer régulièrement l'efficacité des mesures

Checklist sécurité pour le développeur :

Côté technique :
□ HTTPS obligatoire
□ Mots de passe hashés (bcrypt)
□ Données sensibles chiffrées
□ Protection injection SQL/XSS
□ Mise à jour des dépendances

Côté organisation :
□ Accès limités (principe du moindre privilège)
□ Logs des accès aux données
□ Sauvegardes régulières
□ Plan de réponse aux incidents
□ Formation des équipes

En cas de violation de données (articles 33-34)

Une "violation de données" = fuite, perte, accès non autorisé, destruction

Obligations en cas de violation :

72 heures

Notification à la CNIL
(sauf si risque peu probable)

→

Si risque élevé

Notification aux
personnes concernées

→

Toujours

Documenter
l'incident

La notification doit contenir :

- Nature de la violation
- Catégories et nombre de personnes concernées
- Conséquences probables
- Mesures prises ou à prendre

En pratique : préparez un plan de réponse AVANT qu'un incident ne survienne

La CNIL : autorité de contrôle française

Commission Nationale de l'Informatique et des Libertés

Missions principales :

- Informer et protéger les droits des personnes
- Accompagner les organismes dans leur mise en conformité
- Contrôler et sanctionner en cas de manquement
- Anticiper et innover (veille technologique)

Pouvoirs de sanction :

- Avertissement
- Mise en demeure
- Injonction de cesser le traitement
- Amende jusqu'à 20 millions € ou 4% du CA mondial

Ressource utile : www.cnil.fr - Guides, référentiels, FAQ pour les développeurs

Exercice : Analysez cette application

Contexte : Vous développez une application de covoiturage "RideShare"

L'application collecte :

- Nom, prénom, email, téléphone
- Photo de profil
- Géolocalisation en temps réel
- Historique des trajets
- Note et commentaires des utilisateurs
- Informations de paiement (CB)

Questions à analyser :

- Quelles données sont des données personnelles ?
- Y a-t-il des données sensibles ?
- Quelle base légale pour chaque traitement ?
- Quels droits devez-vous permettre d'exercer ?

Réfléchissez 5 minutes

Correction : Application RideShare

1. Données personnelles : TOUTES (identification directe ou indirecte)

2. Données sensibles : Géolocalisation = potentiellement sensible (révèle habitudes, religion...)

3. Bases légales :

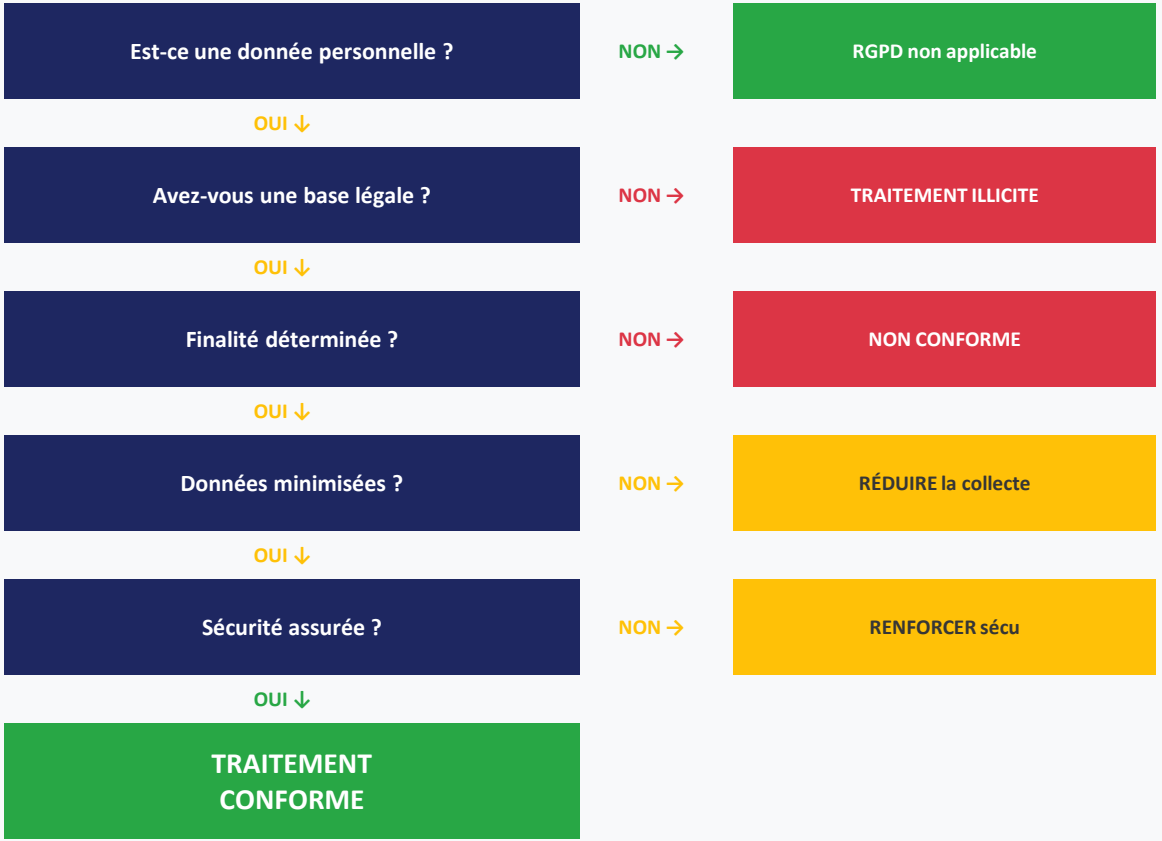
- Nom, email, téléphone → Contrat (Nécessaire au service)
- Géolocalisation temps réel → Contrat + Consentement (Service + données sensibles)
- Historique trajets → Contrat (Nécessaire au service)
- Données CB → Contrat (Paiement du service)
- Photo de profil → Consentement (Non nécessaire au service)

4. Droits à implémenter :

✓ Accès (voir ses données) ✓ Rectification (modifier profil) ✓ Effacement (supprimer compte)
✓ Portabilité (exporter trajets) ✓ Opposition (désactiver géoloc optionnelle)

Bonus : Prévoir une politique de conservation (ex: trajets supprimés après 3 ans)

Arbre de décision : Mon traitement est-il conforme ?



Quiz Wooclap : Testez vos connaissances RGPD

5 questions pour vérifier vos acquis

Q1. Une adresse IP est-elle une donnée personnelle ?

Q2. Quelles sont les 4 caractéristiques d'un consentement valide ?

Q3. Quel est le délai pour notifier une violation à la CNIL ?

Q4. Le droit à l'effacement est-il absolu ?

Q5. Quelle base légale pour envoyer une newsletter ?

Répondez sur Wooclap

Correction du quiz RGPD

Q1. Adresse IP = donnée personnelle ?

OUI - permet l'identification indirecte

Q2. Consentement valide ?

Libre, Spécifique, Éclairé, Univoque (LSEU)

Q3. Délai notification CNIL ?

72 heures maximum

Q4. Droit effacement absolu ?

NON - exceptions (obligation légale, archives...)

Q5. Base légale newsletter ?

Consentement (ou intérêt légitime si client existant)

Ce qu'il faut retenir - Bloc 3

Donnée personnelle :

```
EST_DONNEE_PERSONNELLE = EST_INFORMATION AND (IDENTIFIEE OR IDENTIFIABLE)
```

Traitement licite :

```
TRAITEMENT_LICITE = BASE_LEGALE AND FINALITE_DETERMINEE AND DONNEES_MINIMISEES
```

6 bases légales : Consentement, Contrat, Obligation légale, Intérêts vitaux, Mission publique, Intérêt légitime

Consentement valide :

```
CONSENTEMENT_VALIDE = LIBRE AND SPECIFIQUE AND ECLAIRE AND UNIVOQUE
```

Droits des personnes : Accès, Rectification, Effacement, Limitation, Portabilité, Opposition

Obligations clés : Information, Sécurité, Minimisation, Privacy by Design, Notification violations (72h)

Pour le développeur : intégrez le RGPD dès la conception (Privacy by Design)
Votre code doit permettre l'exercice des droits des utilisateurs

Fin du Bloc 3

TRAITER - Le RGPD et la protection des données

Prochaine étape :

Bloc 4 : SÉCURISER

Cybersécurité et droits en entreprise