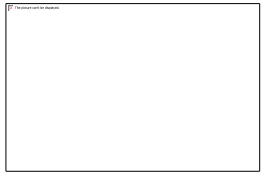
DiGiPort

Protection des données personnelles et de la vie privée - GDPR



Co-funded by the
Erasmus+ Programme
of the European Union

AGITATEUR NUMÉRIQUE
DEPUIS 1999

Фондация на бизнеса за образованието

Co-funded by the
Erasmus+ Programme
of the European Union

Sommaire

DiGiPort

Co-funded by the
Erasmus+ Programme
of the European Union

1.Introduction

Lorsque vous êtes artiste, quelle que soit votre profession, vous vous retrouvez à un moment donné à collecter des données personnelles auprès de clients, de futurs clients, de futurs collaborateurs, d'admirateurs, etc. Ces données personnelles peuvent être consignées dans un cahier, un ordinateur ou être collectées automatiquement par des formulaires en ligne par exemple.

Ce module d'apprentissage permet de mieux comprendre comment protéger les données personnelles et la vie privée dans les environnements numériques ? Comment utiliser et partager des informations personnellement identifiables tout en étant capable de se protéger et de protéger les autres contre les dommages ? Utiliser la " politique de confidentialité " dans les services numériques pour informer sur l'utilisation des données personnelles ? Et ainsi être en conformité avec le Règlement Général de la Protection des Données (RGPD).

Co-funded by the Erasmus+ Programme of the European Union

2.Objectifs d’apprentissage

01

COMPRENDRE le RGPD et ses concepts clés:
- Évolution de la protection des données
- Définition du traitement des données à caractère personnel
- À qui s'applique le RGPD ?

02

CONNAÎTRE les Principes de protection des données :
- Les huit règles d'or pour le traitement des données, la sécurité et la transparence

Co-funded by the Erasmus+ Programme of the European Union

2.Objectifs d'apprentissage

03

SAVOIR DÉFINIR les responsabilités des acteurs :
- Nouvelle logique d'imputabilité
- partage des responsabilités
- Responsabilités spécifiques des sous-traitants
- Sanctions et appels

04

SAVOIR METTRE EN APPLICATION le RGPD
Le DPO et les outils de conformité

Co-funded by the
Erasmus+ Programme
of the European Union

3.Théorie

DiGiPort

01

Évolution de la protection des données - un peu d'histoire pour mieux comprendre

Les débuts : **en France, avec la** loi "Informatique et Libertés".

1978

Directive européenne 95/46/CE adoptée avec les objectifs suivants
- la protection des personnes et la libre circulation des données
- fournir un cadre commun à tous les pays de l'UE en matière de protection des données personnelles - obligation d'adopter une législation par pays + un organe de contrôle indépendant

24 octobre 1995

Nouvelle réglementation européenne qui entre en vigueur dans chaque pays - le **RGPD****

25 mai 2018

Co-funded by the Erasmus+ Programme of the European Union

**RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

3.Théorie

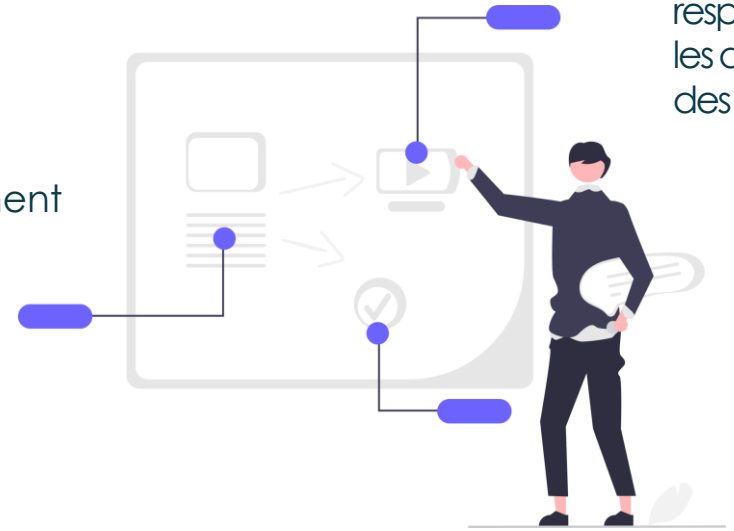
DiGiPort

01

> Les 3 grands principes du RGPD

- une nouvelle logique de responsabilisation de tous les acteurs du traitement des données

- le renforcement quantitatif et qualitatif des individus



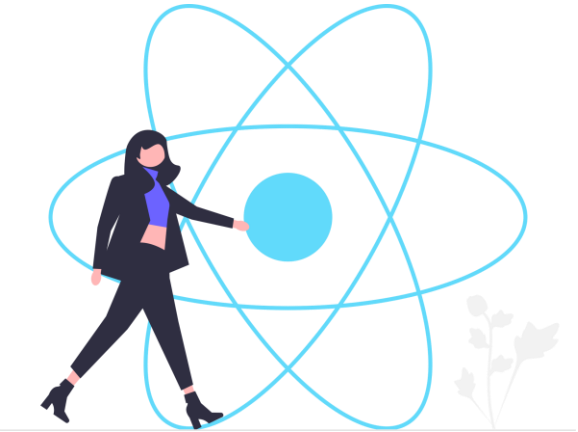
- renforcement du contrôle et de la sanction des structures dédiées au niveau national

Co-funded by the Erasmus+ Programme of the European Union

3.Théorie

01

Avec le développement de la dématérialisation, des objets connectés, des algorithmes, le RGPD garantit un niveau de sécurité adéquat pour les informations traitées et donne aux personnes la possibilité de mieux comprendre et contrôler l'utilisation de leurs données.



Vous le saviez ?

- Les données personnelles sont la base du développement de l'économie numérique.
- Les risques liés à l'utilisation des données personnelles : "95% des propriétaires de smartphones peuvent être ré-identifiés en croisant au moins 4 de leurs localisations géographiques (ex : métadonnées de photos)" Source : Arvind Narayanan citant une étude de YA de Montjoye - Unique dans la foule : les limites de la mobilité humaine en matière de vie privée.

Co-funded by the Erasmus+ Programme of the European Union

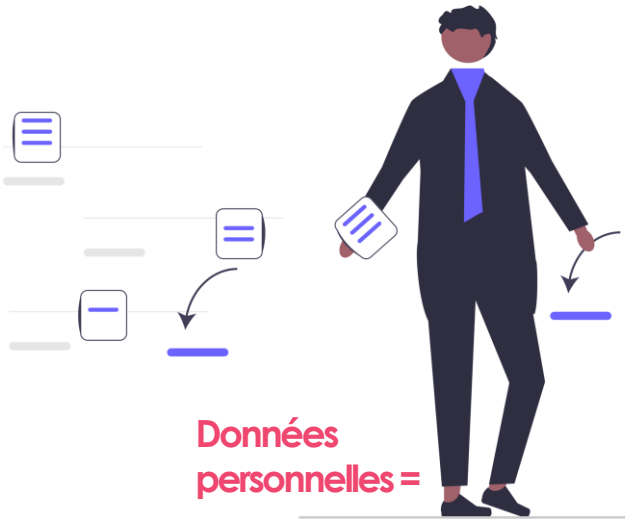
3.Théorie

DiGiPort

01

Les termes "protection des données" et "confidentialité des données" sont souvent utilisés de manière interchangeable, mais il existe une différence importante entre les deux.

La confidentialité des données définit qui a accès aux données, tandis que la protection des données fournit des outils et des politiques pour restreindre réellement l'accès aux données. Les règles de conformité permettent de s'assurer que les demandes de confidentialité des utilisateurs sont prises en compte par les entreprises, et ces dernières sont tenues de prendre des mesures pour protéger les données privées des utilisateurs.



1/ données d'identification indirecte : numéro de client associé à un nom

2/ données d'identification directe : nom, prénom, photo, nom de courriel

3/ toute combinaison d'informations permettant d'identifier la personne : diverses informations sur un compte de réseau social, comme ce que vous aimez, où vous vivez ou travaillez, etc.

Co-funded by the Erasmus+ Programme of the European Union

3.Théorie

01

"Le traitement" : toute opération ou 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, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Co-funded by the
Erasmus+ Programme
of the European Union

3.Théorie

DiGiPort

01

À qui s'applique le RGPD ?

Le RGPD s'applique à toutes les organisations publiques ou privées établies dans l'Union européenne dont les activités s'adressent aux résidents européens. Et ce, qu'elles traitent des données personnelles pour leur propre compte ou en tant que sous-traitant.

Conclusion : si vous êtes un freelance, si vous traitez des données personnelles de citoyens européens et si votre entreprise est basée dans l'UE, vous devez vous conformer aux règles du RGPD !

Vous êtes concerné si vous collectez pour vous-même les données de vos prospects et clients. C'est également le cas si vous participez en tant que prestataire de services à des projets impliquant le traitement de données personnelles (développement de sites web par exemple).

Co-funded by the Erasmus+ Programme of the European Union

3.Théorie

DiGiPort

01

Responsable du traitement et sous-traitant des données

Il est important de comprendre que le RGPD ne s'applique pas au déroulement d'activités strictement personnelles comme le répertoire d'un téléphone, le cloud avec les photos de famille (exception domestique).

Or, le responsable du traitement des données est soumis au RGPD, le cloud, l'opérateur téléphonique, le fabricant de l'enceinte connectée, etc.

Co-funded by the
Erasmus+ Programme
of the European Union

3.Théorie

02

Les principes de protection des données

8 règles d'or résumées en 4 bons réflexes à adopter :

1- ne recueillir que les données réellement nécessaires

2- être transparent

3- penser aux droits des personnes

4- sécuriser les données

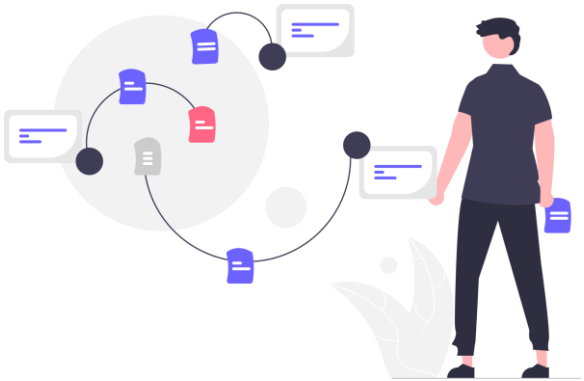
Co-funded by the
Erasmus+ Programme
of the European Union

3.Théorie

02

Principes de protection des données : (voir détails en annexe 1)
La base juridique du traitement : Un traitement ne peut être mis en œuvre que s'il est fondé sur l'une des 6 conditions de conformité à la loi.

1- Finalité du traitement : Les données personnelles recueillies ne peuvent être traitées que pour une finalité précisément définie et légitime - La finalité définit le lien entre les données, les traitements et les organismes qui les mettent en œuvre. Elle définit le champ d'application de leur utilisation.



2- Minimisation des données : Seules les données strictement nécessaires à la réalisation de la finalité peuvent être collectées et traitées - Une donnée est pertinente si elle a un lien direct avec la finalité du traitement.

3- Protection particulière des données sensibles : Les données sensibles ne peuvent être collectées et traitées que dans certaines conditions.

Co-funded by the Erasmus+ Programme of the European Union

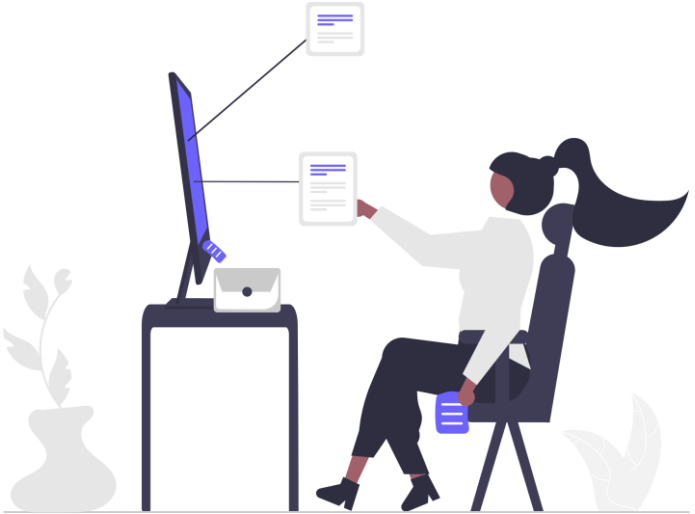
3.Théorie

02

4- Conservation limitée des données : Les données doivent être archivées, effacées ou anonymisées dès que la finalité pour laquelle elles ont été collectées est atteinte : - Obligation de sécurité (Compte tenu des risques, des mesures doivent être mises en œuvre pour assurer la sécurité des données traitées).

5- Transparence : Les individus doivent être informés de l'utilisation de leurs données et de la manière dont ils peuvent exercer leurs droits.

6- Les droits des individus : Les individus ont un certain nombre de droits qui leur permettent de garder le contrôle sur leurs données.



Co-funded by the
Erasmus+ Programme
of the European Union

3.Théorie

DiGiPort

03

Responsabilités des acteurs

> Nouvelle logique de responsabilité : concrètement, tous les acteurs impliqués dans un traitement devront mettre en œuvre et mettre à jour des mesures tant techniques qu'organisationnelles pour garantir à tout moment le respect des grands principes du règlement.

- minimisation

- durée de stockage limitée

- sécurité

- etc.

Co-funded by the
Erasmus+ Programme
of the European Union

3.Théorie

DiGiPort

03

Selon le contexte, tous les acteurs doivent **désigner un délégué à la protection des données, tenir un registre des activités de traitement, appliquer une politique de confidentialité, réaliser une analyse d'impact sur la vie privée**, etc.

Voici les outils obligatoires

- le registre des activités de traitement
- le délégué à la protection des données
- dans certains cas, une analyse d'impact pour certains traitements
- la notification des violations de données dans certaines conditions.

Co-funded by the Erasmus+ Programme of the European Union

3.Théorie

DiGiPort

03

Le partage des responsabilités :

1/2
Lorsque deux ou plusieurs responsables du traitement définissent conjointement les finalités et les moyens du traitement, ils sont des responsables conjoints du traitement, ils sont des responsables conjoints du traitement. Dans ce cas, les responsables conjoints du traitement doivent définir leurs obligations respectives par contrat.

- Responsabilités spécifiques des sous-traitants : Les organisations qui traitent des données personnelles pour le compte de leurs clients ont des responsabilités définies par le GDPR.

-> fournisseurs de services informatiques (hébergement, maintenance ...)
-> Entreprises de services numériques ou anciennement sociétés de services et d'ingénierie informatique (SSII) qui effectuent des traitements de données.
...

Co-funded by the
Erasmus+ Programme
of the European Union

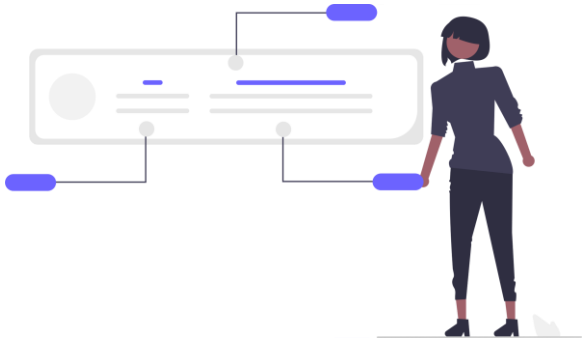
3.Théorie

03

2/2

-> Sociétés offrant des services de télésurveillance
-> les agences de marketing ou de communication qui traitent des données personnelles pour le compte de leurs clients
-> Prestataires de services de paie

Les responsables de traitement, quant à eux, doivent être attentifs aux conditions dans lesquelles ils font appel à un prestataire de services : la protection des personnes concernées doit être assurée tout au long de la chaîne d'externalisation.



Co-funded by the
Erasmus+ Programme
of the European Union

3.Théorie

DiGiPort

03

Sanctions et recours

RECOURS : Plaintes auprès d'une autorité de contrôle.

Toute personne qui considère que le traitement des données personnelles la concernant constitue une violation du GDPR peut déposer une plainte auprès d'une autorité de contrôle.

Il peut s'agir de l'autorité de l'État membre.
- où se trouve la résidence habituelle de l'individu
- où se trouve son lieu de travail
- où la violation s'est produite.

Co-funded by the
Erasmus+ Programme
of the European Union

3.Théorie

DiGiPort

03

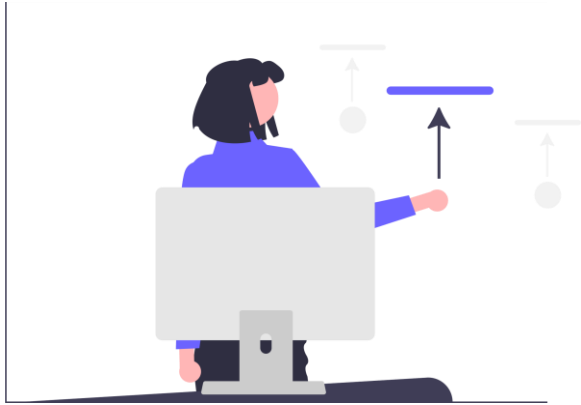
Graduation des amendes administratives

Le montant maximal des amendes administratives diffère en fonction de la gravité de l'infraction.

Le RGPD prévoit à l'article 83 que l'organisme indépendant du pays peut décider d'imposer une amende allant jusqu'à .

- soit 10 millions d'euros ou 2% du chiffre d'affaires mondial

- 20 millions d'euros ou 4 % du chiffre d'affaires mondial



Co-funded by the
Erasmus+ Programme
of the European Union

3.Théorie

04

Le DPO et les outils de conformité

> Le DPO - interne ou externe à temps plein ou partiel - il peut être partagé. Doit être formé mais aucune certification n'est requise.

Ses tâches .

1-Informer et conseiller l'organisation
2-Contrôle de la conformité
3- Agir en tant qu'interface entre son organisation, l'organisme national dédié au RGPD et les personnes concernées.

Le DPO est obligatoire s'il s'agit d'un service public, ou d'une entreprise privée qui traite beaucoup de données personnelles, ou d'une organisation qui traite des données personnelles sensibles. Le DPD n'est pas responsable de toute violation.

Co-funded by the Erasmus+ Programme of the European Union

3.Théorie

Le registre de données

Un registre des activités de traitement doit être mis en place par chaque responsable de traitement ou sous-traitant.
C'est un outil essentiel dans les opérations de conformité, il permet d'identifier C'est un outil essentiel dans les opérations de conformité, il permet d'identifier les activités de traitement, et en même temps, d'avoir une vue d'ensemble de ce qui est fait avec les données personnelles dans les organisations.

Le RGPD exige que le registre soit sous forme écrite. Son format est libre et peut être sous forme papier ou électronique.

Co-funded by the
Erasmus+ Programme
of the European Union

3.Théorie

04

Le registre est un document d'inventaire et d'analyse, qui doit refléter la réalité des traitements et permettre d'identifier précisément

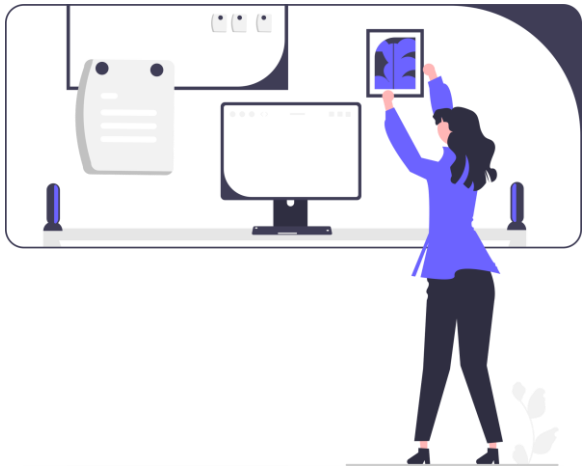
- les parties prenantes (représentant, sous-traitants, responsables conjoints du traitement, etc.) impliquées dans le traitement des données

- les catégories de données traitées ce à quoi servent les données

- qui accède aux données et à qui elles sont communiquées

- la durée de conservation des données

- comment il est sécurisé



Co-funded by the
Erasmus+ Programme
of the European Union

3.Théorie

DiGiPort

04

Les entreprises de moins de 250 salariés bénéficient d'une dérogation. Elles ne sont autorisées à inscrire au registre que les traitements suivants

- les traitements récurrents (par exemple, la gestion des salaires, la gestion des clients, prospects et fournisseurs, etc.)

- les traitements susceptibles d'entraîner un risque pour les droits et libertés des personnes (par exemple, les systèmes de géolocalisation, la vidéosurveillance, etc.)

- les traitements portant sur des données sensibles (par exemple, données sur la santé, infractions, etc.).

Co-funded by the
Erasmus+ Programme
of the European Union

3.Théorie

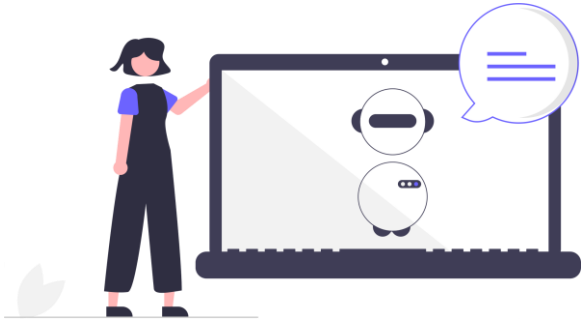
DiGiPort

04

Exemples de violations de données :

- Un pirate accède au code source d'un site web et écrase l'affichage du formulaire de paiement afin de récupérer les coordonnées bancaires saisies tout en permettant le paiement, de sorte que ni l'utilisateur ni l'éditeur du site ne se rendent compte du vol.

- Une organisation spécialisée dans le traitement des patients atteints de maladies graves ne parvient pas à sauvegarder plus de mille personnes lors de l'envoi d'une enquête.



Co-funded by the
Erasmus+ Programme
of the European Union

3.Théorie

Délais de notification

Si l'incident constitue un risque pour la vie privée des personnes concernées, l'organisation doit en informer l'organisme compétent dans le pays où elle est enregistrée.

> Code de conduite et certification

Les codes de conduite et les certifications sont des vecteurs de conformité. Le GDPR appelle à l'élaboration de codes de conduite et/ou de systèmes de certification afin de faciliter l'application des dispositions du règlement par les responsables du traitement et les sous-traitants. et les sous-traitants.
Ils s'adressent à tous les publics professionnels, pour les petites et grandes entreprises.

Co-funded by the
Erasmus+ Programme
of the European Union

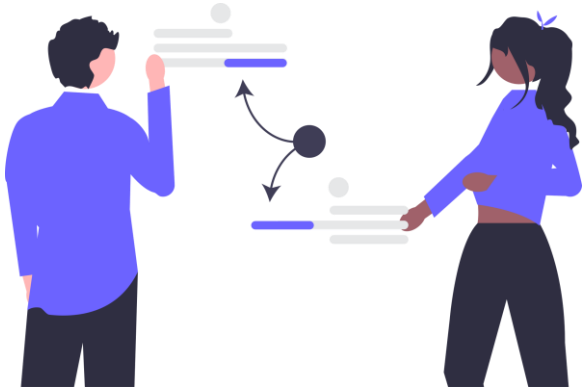
3.Théorie

DiGiPort

04

Les codes de conduite sont des aides utiles à la conformité des organisations, car ils sont adaptés à leur secteur d'activité.

La certification des produits, processus, services et compétences des délégués est un atout important pour une organisation dans ses relations avec ses partenaires ou avec les personnes concernées par le traitement des données en question.



Co-funded by the
Erasmus+ Programme
of the European Union

4.Exemples/Bonnes pratiques

DiGiPort

https://www.blogdumoderateur.com/conformite-rgpd-bonnes-pratiques/
Extrait d'un article (FR) d'un spécialiste du RGPD

Jérôme de Mercey, co-fondateur de Dastra et ancien agent de la CNIL, partage ses conseils aux entreprises.

(...) **Quels sont les départements les plus touchés au sein des organisations ?**
Le service commercial/marketing sera en première ligne en raison de l'activité de prospection commerciale qui peut générer de nombreuses plaintes de la part de prospects de plus en plus alertés par l'utilisation des données. Le service RH est historiquement très touché car les données traitées sont très sensibles et souvent demandées dans le cadre de litiges avec les salariés.

Co-funded by the
Erasmus+ Programme
of the European Union

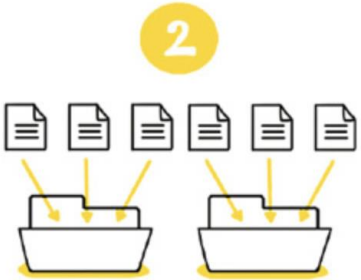
Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

4.Exemples/Bonnes pratiques

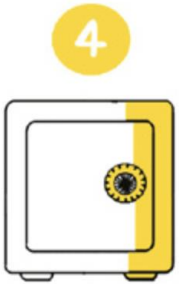
RGPD- Agir en quatre étapes (Source : https://www.cnil.fr/fr/rgpd-par-ou-commencer)

Tenir un registre du traitement de vos données



Trier vos données

Respecter les droits des personnes



Gardez vos données sécurisées

Co-funded by the Erasmus+ Programme of the European Union

DiGiPort

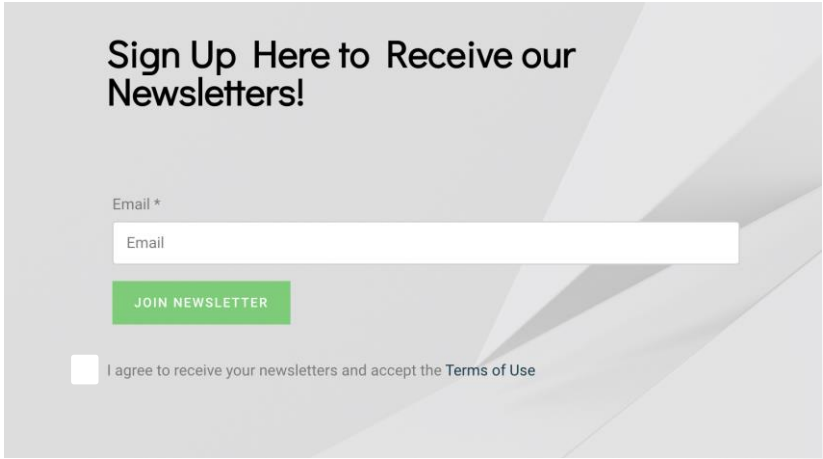
4.Exemples/Bonnes pratiques

Article avec les meilleures pratiques
9 éléments essentiels et 3 meilleures pratiques

https://cloudian.com/guides/data-protection/data-protection-policy-9-things-to-include-and-3-best-practices/

Un exemple - Site web du projet DIGIPORT

Insérer une case à cocher pour le consentement dans vos formulaires de contact ou vos abonnements à la newsletter
–>>>>>



4.Exemples/Bonnes pratiques

DiGiPort

Extrait d'un autre article, celui d'un spécialiste du RGPD
https://www.blogdumoderateur.com/conformite-rgpd-bonnes-pratiques/

Jérôme de Mercey, co-fondateur de Dastra et ancien agent de la CNIL, partage ses conseils aux entreprises.

(...) **Comment mettre en place une bonne gestion des cookies sur un site web ? Quelles sont vos recommandations dans ce domaine ?** Les cookies sont un sujet complexe car cela ne s'arrête pas aux seuls cookies. Il faut aussi voir tout ce qui transite sur le réseau et être capable de comprendre l'objectif et les destinataires de chaque requête. Il faut donc interroger les "sachants" : les équipes de développement du site web et les interpeller sur ce qui est déposé, lu et demandé lors de la navigation sur le site. Vous devez ensuite traduire ces comportements et les qualifier au regard de la réglementation, mettre en place un bandeau de cookies et demander le consentement des internautes si cela est justifié. Le plus simple est d'utiliser un outil spécialisé ou de se faire conseiller pour la mise en place de ce bandeau. Vous pouvez également lire les lignes directrices de la CNIL sur le sujet qui sont très explicites. (...)

Co-funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

4.Exemples/Bonnes pratiques

12 bonnes pratiques

https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

1. formaliser l'engagement de la direction
La première étape, essentielle, consiste à formaliser l'engagement de la direction. En effet, c'est le PDG qui est responsable du traitement. Il représente donc l'entreprise en cas d'action en justice, qu'il s'agisse d'une PME ou d'une grande entreprise.

2. communiquer le contenu du RGPD
Il est ensuite nécessaire de diffuser l'information sur le règlement au sein de l'entreprise, de manière claire et compréhensible, afin de sensibiliser les employés.

Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

4.Exemples/Bonnes pratiques

12 Bonnes pratiques
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

3. former les employés
Une fois la phase de communication terminée, l'entreprise peut alors entreprendre la formation de ses employés et assurer la mise à jour des différents documents faisant référence au traitement des données (contrats, documents RH).

4. tenir un registre des opérations de traitement
L'entreprise doit également tenir un registre des activités de traitement, ce qui constitue une obligation pour le responsable du traitement. En cas de traitement nécessitant un suivi régulier ou de traitement de données volumineuses, elle doit désigner un délégué à la protection des données ('DPD''), avec la possibilité de recourir à un DPD externe si nécessaire.

DiGiPort

4.Exemples/Bonnes pratiques

12 Bonnes pratiques
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

5.mener des évaluations d'impact sur la vie privée
L'entreprise doit étudier l'impact sur la vie privée des différents traitements effectués sur les données personnelles de ses clients et employés.

6. établir un plan d'audit du traitement
L'entreprise doit également mettre en place un plan d'audit du traitement afin de s'assurer que celui-ci reste dans le cadre autorisé par la réglementation. Une vigilance particulière est requise pour les transferts de données hors de l'Union européenne.

Co-funded by the
Erasmus+ Programme
of the European Union

4.Exemples/Bonnes pratiques

DiGiPort

12 Bonnes pratiques
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

7. permettre le signalement des infractions
L'entreprise doit mettre en place une procédure permettant à toute personne de signaler les violations de données personnelles.

8. être vigilant pour garantir l'exercice des droits
Les entreprises doivent être particulièrement attentives au respect des droits de toute personne sur laquelle elles détiennent des données, qu'il s'agisse de clients ou d'employés, comme le droit à l'oubli.

9. suivi de la conformité dans le temps
Les entreprises doivent surveiller leur politique globale de protection des données au fil du temps.

Co-funded by the
Erasmus+ Programme
of the European Union

4.Exemples/Bonnes pratiques

DiGiPort

12 Bonnes pratiques
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

10. vérification de la conformité du fournisseur
Il est important d'évaluer la conformité des prestataires de services stratégiques et des sous-traitants, notamment ceux qui ont accès aux données de l'entreprise. Les contrats doivent être revus pour inclure un certain nombre de mentions obligatoires, délimitant les usages autorisés.

11. intégration du "Privacy by design" dans les pratiques
Sur le plan technique, il faut veiller à se conformer au RGPD dès la conception de nouveaux services applicatifs, en intégrant le principe de " Privacy by design " dans les pratiques de développement. Ce principe s'applique également si l'entreprise fait développer des applications par un prestataire ou achète des logiciels tiers : elle doit déterminer au plus tôt les données collectées, les traitements, les types de destinataires et la durée de conservation.

Co-funded by the
Erasmus+ Programme
of the European Union

Exemples/Bonnes pratiques

12 Bonnes pratiques
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

12. prévoir un plan de sauvegarde des données
La mise en place d'un plan de sauvegarde des données est également indispensable, avec des mesures de protection appropriées des données personnelles. L'entreprise est en effet tenue d'assurer une sécurité informatique renforcée, avec une obligation, en cas de faille de sécurité, de notifier la CNIL dans les 72 heures et, dans certains cas, les personnes concernées. Pour l'instant, seules 51% des entreprises ont déclaré des incidents au cours des douze derniers mois, ce qui laisse penser qu'il y a un manque à gagner dans ce domaine.

Co-funded by the
Erasmus+ Programme
of the European Union

4.Exemples/Bonnes pratiques

RGPD - Email Marketing -(Source : https://www.cnil.fr/fr/rgpd-par-ou-commencer)

Lorsqu'il s'agit de marketing par courriel, les meilleures pratiques suivantes doivent être mises en place :
- N'utilisez pas de case pré-cochée ou d'autre option par défaut.
- Séparez la déclaration de consentement des autres conditions.
- Formulez les choses différemment : oui, je veux être informé.
- Donner le choix de consentir à des opérations de traitement indépendantes.
- Montrez qu'il est facile de se désabonner et d'exercer ses différents droits.
- S'assurer que le consentement des enfants est obtenu légalement.
- Documenter au mieux l'obtention du consentement
(par exemple, double opt-in).

Co-funded by the
Erasmus+ Programme
of the European Union

5.Quiz

QUELQUES QUESTIONS POUR VOIR CE QUE VOUS AVEZ APPRIS :

1- La consultation des données d'un fichier client est-elle considérée comme un traitement de données personnelles ?
Oui-Non

2- La notion de traitement s'applique-t-elle également aux documents papier ?
Oui-Non

3- Une association culturelle fait généralement remplir à ses membres une fiche de renseignements. Chaque fiche est classée par ordre alphabétique dans un dossier dédié. Le RGPD s'applique-t-il ?
Oui-Non

Co-funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

5.Quiz

QUELQUES QUESTIONS POUR VOIR CE QUE VOUS AVEZ APPRIS :

4-"Nous sommes heureux de vous compter parmi nos nouveaux utilisateurs ! Conformément au RGPD, si vous ne souhaitez pas que votre adresse e-mail soit utilisée à des fins de prospection commerciale, veuillez nous envoyer un e-mail à gdpr@myservice.fr" Cette méthode de recueil du consentement est-elle valable ?
Oui-Non ?

5- La collecte de la date de naissance d'une personne est-elle pertinente pour tout type de traitement ?
Oui-Non ?

Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

5.Quiz

QUELQUES QUESTIONS POUR VOIR CE QUE VOUS AVEZ APPRIS :

6- La collecte de la tranche d'âge doit-elle être obligatoire ou facultative ?
Facultative-Obligatoire

7- La vidéosurveillance doit-elle appliquer le RGPD ?
Oui-Non

8- Consentement ? Doit être :
explicite - univoque - révocable - informé ?

9- Pendant combien de mois les données de la carte bancaire peuvent-elles être archivées suite à un achat en ligne ?
24 mois - 15 mois - 6 mois - 13 mois

Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

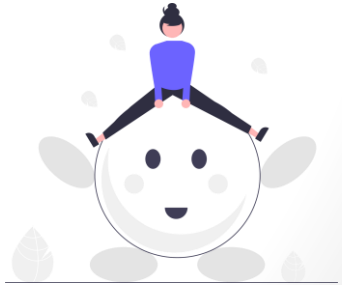
5.Quiz

QUELQUES QUESTIONS POUR VOIR CE QUE VOUS AVEZ APPRIS :

10-Lorsque l'on parle de cryptage des données, de quoi parle-t-on ?
encodage-sauvegarde-chiffrage-dupliclable?

11-Il est possible que l'organisme indépendant du RGPD de chaque pays puisse émettre une amende tarifaire ?
Oui - Non ?

12- Où le RGPD s'applique-t-il ?
Dans l'UE ? - En dehors de l'UE ? Partout ?



Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

6.Références

https://www.cnil.fr/fr/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie

https://www.cnil.fr/fr

https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/

https://globalprivacyassembly.org/

https://www.oecd.org/

https://www.coe.int/fr/web/portal/home

Co-funded by the
Erasmus+ Programme
of the European Union

7.ANNEXES

ANNEXE 1 : La base juridique du traitement : Un traitement ne peut être mis en œuvre que s'il est fondé sur l'une des 6 conditions de licéité (voir détails en annexe 1).

- Finalité du traitement : Les données personnelles recueillies ne peuvent être traitées que pour une finalité précisément définie et légitime - La finalité définit le lien entre les données, les traitements et les organismes qui les mettent en œuvre. La finalité définit le lien entre les données, les traitements et les organismes qui les mettent en œuvre. Elle définit le champ d'application de leur utilisation.
- Minimisation des données : Seules les données strictement nécessaires à la réalisation de la finalité peuvent être collectées et traitées - Une donnée est pertinente si elle a un lien direct avec la finalité du traitement.
- Protection spéciale des données sensibles : Les données sensibles ne peuvent être collectées et traitées que sous certaines conditions

Co-funded by the
Erasmus+ Programme
of the European Union

7.ANNEXES

ANNEXE 1 : La base juridique du traitement : Un traitement ne peut être mis en œuvre que s'il est fondé sur l'une des 6 conditions de licéité.

- Conservation limitée des données : Les données doivent être archivées, effacées ou anonymisées dès que la finalité pour laquelle elles ont été collectées est atteinte : - Obligation de sécurité (Compte tenu des risques, des mesures doivent être mises en œuvre pour assurer la sécurité des données traitées).
- Transparence : Les personnes doivent être informées de l'utilisation de leurs données et de la manière dont elles peuvent exercer leurs droits.
- Droits des personnes : Les personnes ont un certain nombre de droits qui leur permettent de garder le contrôle sur leurs données.

7.ANNEXES

DiGiPort

ANNEXE 1

Minimisation des données (Seules les données strictement nécessaires à la réalisation de la finalité peuvent être collectées et traitées - Une donnée est pertinente si elle est directement liée à la finalité du traitement - Pour vérifier si vous respectez le principe de minimisation. Pour vérifier si vous respectez le principe de minimisation, posez-vous les bonnes questions Quelle est ma finalité ? Quelles sont les données essentielles pour atteindre cette finalité ? pour atteindre cette finalité ? Ai-je le droit de collecter ces données ? Ai-je fait une distinction claire entre les données obligatoires et les données facultatives ?

Protection spéciale des données sensibles (Les données sensibles ne peuvent être collectées et traitées que sous certaines conditions - Les données sensibles sont celles qui révèlent ou concernent : - l'origine raciale ou ethnique - les opinions politiques - les convictions philosophiques ou religieuses - l'appartenance syndicale - la santé (physique ou mentale) - la vie sexuelle ou l'orientation sexuelle - les données génétiques - les données biométriques permettant d'identifier une personne physique de manière unique).

Co-funded by the
Erasmus+ Programme
of the European Union

7.ANNEXES

DiGiPort

ANNEXE 1

Conservation limitée des données (Les données doivent être archivées, supprimées ou anonymisées dès que la finalité pour laquelle elles ont été collectées est atteinte - Les organisations doivent être en mesure de justifier le cycle de vie des données qu'elles détiennent : besoins correspondant aux différentes phases, données et durée de conservation retenues pour chacune).

Obligation de sécurité (Compte tenu des risques, des mesures doivent être mises en œuvre pour assurer la sécurité des données traitées - UN MOT DE PASSE CONCRET I Un bon mot de passe doit contenir 12 caractères, d'au moins 4 types différents : minuscules, majuscules, chiffres et caractères spéciaux. Il peut être plus court si votre compte est équipé de dispositifs de sécurité supplémentaires !) - La transparence (Les personnes doivent être informées de l'utilisation de leurs données et des moyens d'exercer leurs droits) - Les droits des personnes (Les personnes disposent d'un certain nombre de droits qui leur permettent de garder le contrôle de leurs données).

Co-funded by the Erasmus+ Programme of the European Union

7.ANNEXES

DiGiPort

ANNEXE 1

Transparence (Les personnes doivent être informées de l'utilisation de leurs données et de la manière dont elles peuvent exercer leurs droits) - Droits des personnes (Les personnes ont un certain nombre de droits qui leur permettent de garder le contrôle sur leurs données - La limitation du traitement ne peut être demandée que dans l'une des 4 situations suivantes .

-lorsque la personne a exercé son droit de rectification.
Le droit à la limitation s'applique pendant que le responsable du traitement vérifie l'exactitude des données personnelles concernées. les données personnelles concernées (il dispose d'un mois)

- Lorsque la personne a exercé son droit d'opposition.
Le droit à la limitation s'applique pendant la durée nécessaire pour déterminer si les intérêts légitimes du responsable du traitement prévalent sur ceux de la personne concernée.

Co-funded by the
Erasmus+ Programme
of the European Union

7.ANNEXES

DiGiPort

ANNEXE 1

- lorsque les données sont sur le point d'être supprimées alors qu'elles sont encore nécessaires
à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice

- lorsque le traitement est illicite mais que la personne concernée préfère la limitation plutôt que l'effacement des données. Le GDPR permet donc aux responsables du traitement de ne pas donner suite à une demande)

Le GDPR met en place des mécanismes pour compenser l'absence de protection des données dans certains pays tiers. L'objectif est de faire en sorte que la "bulle de protection" suive les données à tout moment.

Co-funded by the
Erasmus+ Programme
of the European Union