

Privacy By Design (PbD)

Pour que la technique vous aide à respecter le RGPD :
la méthodologie NEXT avocats

Novembre 2021

NEXT avocats – www.next-law.fr
15 rue du Temple – 75004 Paris
contact@next-law.fr – 01 75 43 86 23

Le « Privacy by Design », concrètement → Concevoir

1

- Quel est l'article du RGPD concerné ?



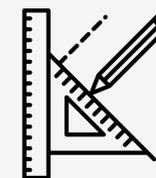
2

- Quelles est l'exigence posée par l'article ?



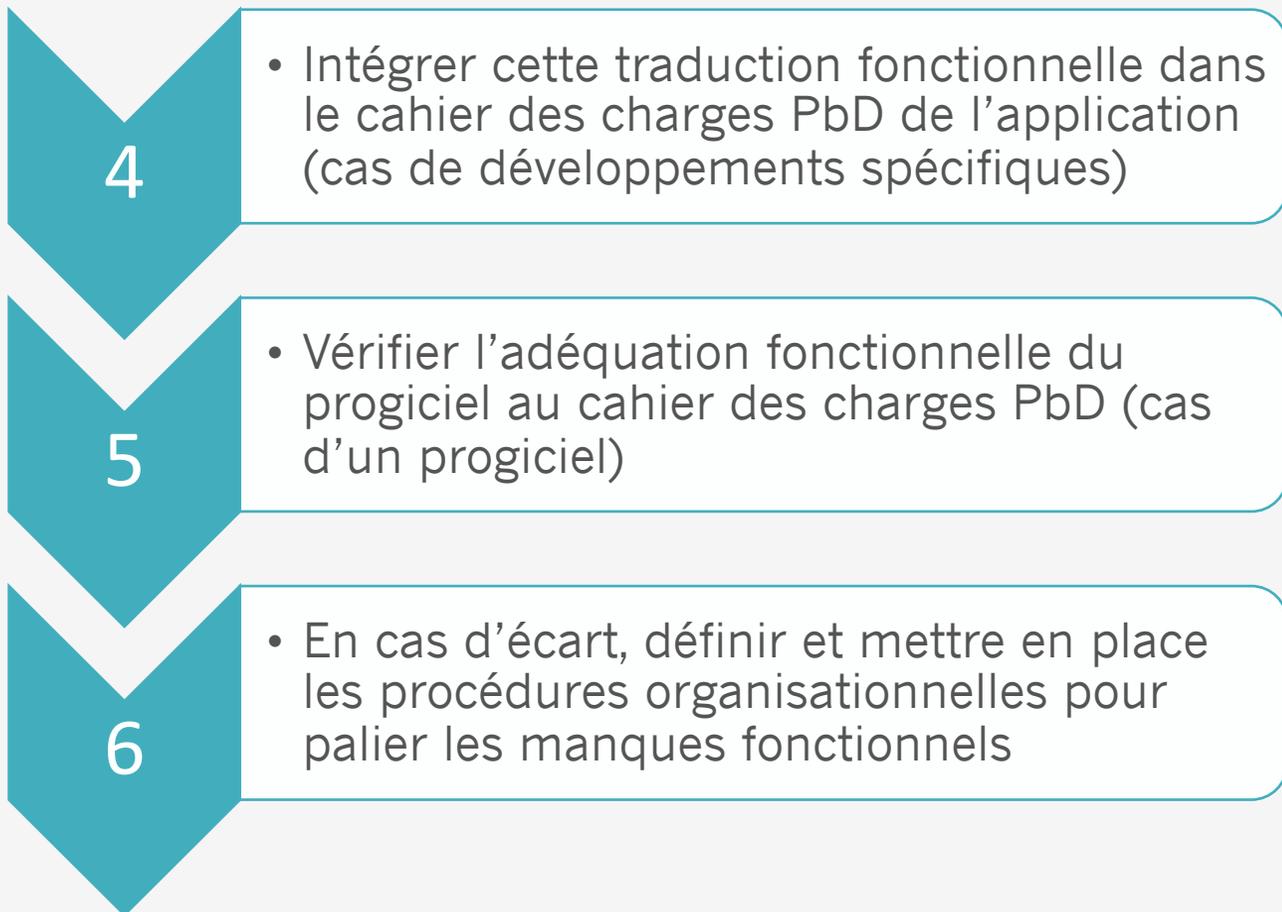
3

- Quelle est la traduction fonctionnelle et/ou technique de l'exigence ?



Le « Privacy by Design », concrètement → Formaliser

NEXT



Le « Privacy by Design », concrètement → Valider

NEXT

4

- Intégrer les exigences fonctionnelles PbD au cahier de recette



5

- Nommer un responsable chargé d'approuver toute évolution fonctionnelle de ces critères



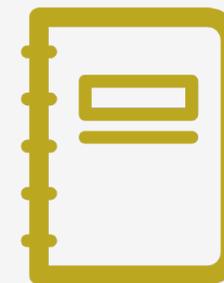
6

- Recommencer le cycle pour toute évolution fonctionnelle



Le cahier des charges « Privacy by Design » :

notre exemple pour
les étapes 1 à 3 (Concevoir)



Fonctions de l'application liées à la minimisation et à la pertinence des données collectées

NEXT

1	2	3
Art. 5.1.b	Les données sont collectées pour des finalités déterminées	<i>Exemple : L'application ne doit pas permettre la modification ou l'ajout d'algorithmes de traitements automatiques sur les données sans qu'un responsable RGPD habilité ait donné son aval.</i>
Art. 5.1.c	Les données collectées sont limitées à ce qui est nécessaire au regard des finalités	<i>Exemple : L'application ne doit pas permettre la modification ou l'ajout de champs de données sans qu'un responsable RGPD habilité ait donné son aval.</i>
Art. 5.1.d	Les données sont tenues à jour	<i>Exemple : Une date d'obsolescence doit pouvoir être programmée pour chaque champ de données (paramètre de durée ou de date).</i>



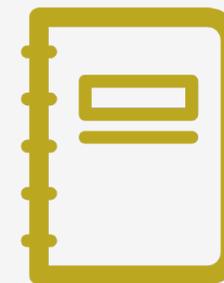
Fonctions de l'application liées à la limitation de la durée de conservation des données collectées



1	2	3
Art. 5.1.e	Les données sont conservées pendant une durée n'excédant pas la durée nécessaire au regard des finalités pour lesquelles elles sont traitées	<i>Exemple : Chaque champ de donnée doit être associé à une durée de conservation (paramètre de durée ou de date).</i>
		<i>Exemple : Des alertes automatiques vers un utilisateur habilité et/ou la personne concernée doivent être effectuées une fois la durée de conservation atteinte.</i>
		<i>Exemple : Une fonction de suppression ou d'archivage ou de pseudonymisation doit pouvoir être déclenchée automatiquement et/ou par un utilisateur habilité et/ou la personne concernée une fois la durée maximale de conservation atteinte.</i>



...Poursuivre le cahier des charges
« privacy by design » pour chacun des
domaines fonctionnels « RGPD » suivants



Fonctions liées à la sécurité et la confidentialité des données collectées



- Art. 5.1.f : Les données sont traitées de façon à garantir leur sécurité.
- Art. 5.1.f : Les données sont protégées contre le traitement non autorisé
- Art. 5.1.f : La confidentialité des données doit être assurée

Fonctions liées à la préservation de la preuve du consentement lorsque celui-ci fonde le traitement



- Art. 6.1.a / Art. 7.1 : La personne concernée consent au traitement de ses données
- Art. 7.3 : La personne concernée doit pouvoir retirer son consentement

Fonctions liées à l'exercice des droits des personnes concernées



- Art. 15.3 : La personne concernée peut obtenir une copie des données la concernant faisant l'objet d'un traitement
- Art. 16 : La personne concernée a le droit d'obtenir la rectification de ses données
- Art. 17.1 : La personne concernée a le droit d'obtenir l'effacement de ses données
- Art. 20 : La personne concernée dispose d'un droit à la portabilité de ses données
- Art. 21.1 : La personne concernée a le droit de s'opposer au traitement de ses données
- Art. 21.2 : La personne concernée a le droit de s'opposer au traitement de ses données à des fins de prospection
- Art. 21.5 : La personne concernée doit pouvoir exercer son droit d'opposition directement par une fonctionnalité de la solution lorsqu'il s'agit d'un service de communication électronique (site web, smartphone, etc.)
- Art. 22 : La personne concernée ne doit pas faire l'objet d'une décision produisant des effets juridiques la concernant qui serait fondée exclusivement sur un traitement automatisé (ex. profilage).



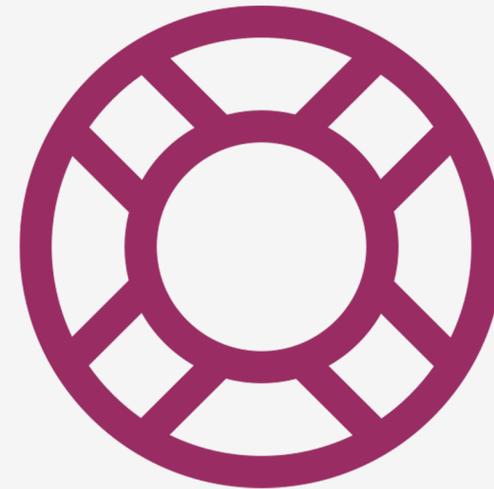
Votre mise en conformité RGPD

Vous ne savez pas faire ?

Vous n'avez pas le temps de le faire ?

Vous n'avez personne pour le faire ?

Nous savons le faire et nous pouvons vous aider



NEXT avocats: distinctions accordées par les guides juridiques et la presse spécialisée

NEXT

**BEST
LAWYERS
2022**

CATEGORIES

Droit des Technologies de
l'Information

Droit de la Propriété
Intellectuelle

Droit des Médias

Droit des données personnelles

Droit des Technologies

**LEGAL 500
EMEA
2020**

CATEGORIES

Informatique & Internet

Données personnelles

**LEADERS LEAGUE
& DECIDEURS
MAGAZINE 2021**

CATEGORIES

Données personnelles

Internet

Droit de la publicité

Spectacles vivants

Droit de la musique





DIGITAL & CREATIVE BUSINESS LAW

INFORMATIQUE INTERNET RESEAUX SOCIAUX E-COMMERCE

DONNEES PERSONNELLES RGPD DATA PRIVACY

TRANSITION DIGITALE ACTIFS NUMERIQUES

CREATION SPECTACLES DIVERTISSEMENT AUDIOVISUEL

L'actualité du droit du numérique
et de la création décryptée. Suivez-nous :



twitter.com/NextAvocats



www.linkedin.com/company/next-avocats/



www.instagram.com/next_avocats/