WordCamp Lyon 2022

Embarcadere-Public
Embarcadere!

Comment le RGPD peut influer sur le périmètre technique d'un projet web ?

Florian Chambolle & Flore Châtelet

40 min • RGPD

PLANNING

Le RGPD en 2022

Montée en puissance du numérique depuis 1978

Les mesures techniques et organisationnelles de la protection des données imposées aux personnes morales

Les menaces plus virulentes : compromission des ressources applicatives, vol de données, déni de service

Sanctions parfois lourdes en cas de non respect et de violation des données

Le RGPD en 2022

Objectifs du RGPD :

- **Harmoniser les mesures de protection des données au travers de l'UE**
- **Eviter les risques de violation de données**
- **Responsabiliser les entreprises**
- **Respecter les droits des personnes concernées**

Cela passe impérativement par :
-> Imposer la sécurisation des sites et plateformes, cibles préférées des hackers et portes d'entrée des attaques malveillantes

Un peu d'événements

- infogreffe : compte utilisateur - 250 k€ - défaut de respect des durées de conservation et de sécurité des données

- Dedalus Biologie : commercialisation de solutions logicielles pour les laboratoires d'analyse - 1,5 M€ - fuite de données médicales - blocage du site - manque de sécurité des données - manquement à l'obligation du ST de respecter les instructions du RT sur la migration du volume de données

PLANNING

Un peu d'événements

- **Accor : réservation hôtelière 600 k€ - manquement à l'obligation d'informer les personnes concernées, de respecter les droits des personnes concernées, défaut de recueil du consentement pour l'envoi d'une newsletter…**

- **Amazon Europe Core : 35 M€ non-respect de la législation sur les cookies**

Un projet de A à Z

1. Recueil du besoin client
2. Briefs
3. Ateliers
4. Élaboration du cahier des charges et du plan fonctionnel
5. Production
6. Recettes
7. Mise en production

PLANNING

WordCamp Lyon 2022

Embarcadere-Public
Embarcadere!

Un projet web, du recueil du besoin client à la mise en production

PLANNING

Le besoin de ce client... parlons-en

Un site vitrine avec :

- une home
- des pages internes
- une page de contact

Le besoin de ce client… ne s’arrêtait pas là

il fallait aussi :

- **un espace client sur un sous-domaine type clients.monsite.fr**

“Et c’est là que ça se corse”

- Napoléon

Focus sur les fonctionnalités de notre projet

PLANNING

Le site vitrine

- blocs de texte
- blocs images + textes
- ...
- formulaire de contact

Le site vitrine... alerte !

- Site sécurisé
- Droit à l'image ou droit de propriété
- Formulaire de contact
- Bandeau de cookies
- Gestion des consentements
- Politique de gestion des cookies
- Mentions légales

L’espace client

Un fonctionnement en silos :

- **plusieurs entreprises clientes sur le même espace**
- **les utilisateurs de l’entreprise A ne peuvent voir que leurs collègues de la même entreprise**
- **les consultants et administrateurs peuvent voir tous les profils**

L’espace client… alerte !

- Conditions générales d’utilisation
- Politique de protection des données : quoi, qui, où, comment, quand ?

-> Vous devez informer les personnes concernées du sort de les données qu’elles vous confient

L’espace client

5 profils d’utilisateurs :

- **administrateur**
- **consultants**

- **client responsable du compte entreprise**
- **client middle manager**
- **client utilisateur restreint**

L’espace client… alerte !

- Déterminer les rôles
- Déterminer les accès
- Gérer les habilitations
- Engagement de confidentialité des salariés

L'espace client

Parcours des utilisateurs consultants :

- connexion à leur espace consultant
- remplissage de leur profil consultable par les clients
- accès à leur agenda
- gestion de leurs disponibilités / indisponibilités
- gestion des réservations

L'espace client

Parcours des utilisateurs utilisateur restreint :

- connexion à leur espace client
- remplissage de leur profil consultable par les consultants et les autres personnes de leur entreprise
- demandes de réservations de séances
- accès à leurs réservations

PLANNING

L’espace client

Parcours des utilisateurs middle manager :

- connexion à leur espace client
- remplissage de leur profil consultable par les consultants et les autres personnes de leur entreprise
- demandes de réservations de séances
- accès à leurs réservations
- validation des demandes des utilisateurs restreints
- utilisation des crédits de l’entreprise

PLANNING

L’espace client

Parcours des utilisateurs responsable du compte entreprise :

- connexion à leur espace client
- remplissage de leur profil consultable par les consultants et les autres personnes de leur entreprise
- demandes de réservations de séances
- accès à leurs réservations
- validation des demandes des utilisateurs restreints
- utilisation des crédits de l’entreprise
- répartition des crédits de l’entreprise entre différents middle managers

PLANNING

L’espace client… alerte !

- Mot de passe suffisamment complexe
- Profils consultants et utilisateur restreint “juste ce qu’il faut”
- Portabilité des données

Au final...

Les conséquences

... de la prise en compte du RGPD pendant le projet :

- **un périmètre technique à revoir**
- **plus de temps passé sur le projet**
- **diminution de la marge**

Et encore des conséquences...

- Notoriété du client difficile
- Exposition aux menaces
- Site moins responsable

WordCamp Lyon 2022

Embarcadere-Public
Embarcadere!

Comment aurions-nous pu faire autrement ?

PLANNING

Un projet de A à Z… en passant par RGPD

1. Recueil du besoin client
2. Briefs
3. Ateliers
4. Concertation avec un expert en protection des données
5. Élaboration du cahier des charges et du plan fonctionnel
6. Production
7. Recettes
8. Mise en production

PLANNING

WordCamp Lyon 2022

Un projet de A à Z...
en passant par le RGPD

Rappel de 4 règles d'hygiène :

- **Sécurité des sites et applications web à prendre en compte dès le début**
- **Intégrité du comportement de l'application côté client**
- **Configurer l'infrastructure d'hébergement**
- **Permettre de détecter les vulnérabilités et attaques éventuelles (audit)**

PLANNING

Pour vos clients...

...soyez vous-même conforme au RGPD

Eh oui, au regard du RGPD, suivant le cas vous serez Responsable de traitement, ou Sous-traitant ou encore Co-responsable de traitement.

-> et vous avez des obligations d'informations et un devoir de conseil.

"Si vous ne prenez pas soin de vos clients, votre concurrent le fera"
Bob Hooey, auteur a succès

WordCamp Lyon 2022

Embarcadere-Public
Embarcadere!

Flore Chatelet

Fondatrice d'Aporia
et de Mon Audit RGPD

aporiasas.fr
mon-audit-rgpd.fr

Florian Chambolle

Co-fondateur de
l'Agence 810 et de fourty

agence810.fr
getfourty.io

PLANNING

WordCamp Lyon 2022

Embarcadere-Public
Embarcadere!

Merci à toutes et à tous

Des questions ?

PLANNING