SAE 3.01
Développement d'un site de E-Commerce

Analyse d'impact
Site LeRoiMerlin

ALLEMANE Axel - ROMA Quentin - LE DONNE Antonin - RIBEIRO VAUR Nino - OLIVENCIA Eliot

Sommaire

1. Présentation générale du traitement

1.1 Contexte du projet

Le projet **LeRoiMerlin** est un site de commerce électronique B2C destiné à la vente de produits physiques à destination de clients situés en France.
Le site permet la consultation libre du catalogue, mais impose la création d'un compte client pour toute commande.

Le site traite des **données à caractère personnel**, notamment lors :

- de la création d'un compte client
- du passage de commande
- du paiement
- de la livraison
- de la gestion des avis

Bien que l'analyse d'impact ne soit pas systématiquement obligatoire pour un e-commerce classique, le client a souhaité qu'une **AIPD préventive** soit réalisée afin d'anticiper les risques et de garantir la conformité au RGPD.

1.2 Finalités des traitements

Les traitements de données personnelles ont pour finalités :

- la gestion des comptes clients
- la gestion des commandes et livraisons
- la gestion des paiements (y compris l'enregistrement optionnel des cartes bancaires)
- la gestion du programme de fidélité
- la gestion des avis clients
- l'amélioration du service et de la sécurité du site.

1.3 Enjeux et activités sensibles

Les activités les plus sensibles en matière de protection des données sont :

- le **paiement en ligne**, en particulier le stockage optionnel des données de carte bancaire
- la **gestion des comptes clients** (authentification, mots de passe)
- la **livraison**, impliquant des données d'adresse postale
- la conservation des **cookies de session**.

Ces traitements présentent des risques en cas de compromission (fraude, usurpation d'identité, atteinte à la vie privée).

2. Étude des principes fondamentaux du RGPD

2.1 Nécessité et proportionnalité des traitements

Les traitements de données personnelles mis en œuvre par le site **LeRoiMerlin** sont strictement nécessaires à la réalisation des finalités définies.

Les données collectées lors de la création d'un compte client (nom, prénom, adresse email, mot de passe) sont indispensables à l'identification de l'utilisateur et à la gestion de son espace personnel. Les données relatives aux commandes et à la livraison (adresse postale, historique des commandes) sont nécessaires à l'exécution du contrat de vente et au respect des obligations légales et comptables.

Aucune donnée excessive ou non pertinente n'est collectée. Le principe de minimisation des données est respecté : seules les informations strictement nécessaires au fonctionnement du service sont traitées.

Durées de conservation appliquées :

- Données de compte client : 3 ans après la dernière connexion
- Factures et historique de commandes : 10 ans (obligation légale comptable)
- Adresse de livraison : 1 an après la livraison effective
- Carte bancaire enregistrée : jusqu'à révocation du consentement par le client
- Cookies de session : fermeture du navigateur ou 24h d'inactivité
- Cookies statistiques : 13 mois maximum (recommandation CNIL)

Le traitement des données de paiement repose sur un consentement explicite. Le CVV n'est jamais stocké, conformément aux normes PCI-DSS.

Ainsi, les traitements réalisés sont proportionnés, licites et conformes aux exigences de l'article 5 du RGPD.

2.2 Respect des droits des personnes concernées

Le site LeRoiMerlin met en œuvre des mesures permettant de garantir le respect des droits des personnes concernées, conformément au RGPD.

Les utilisateurs sont informés de manière claire et transparente sur les traitements réalisés lors de la création du compte et au moment du paiement. Le recueil du consentement est explicite lorsque requis, notamment pour l'enregistrement des données de carte bancaire.

Les clients disposent de droits d'accès, de rectification et de suppression de leurs données personnelles via leur espace client. Ils peuvent également demander la suppression de leur carte bancaire enregistrée à tout moment.

Les données sont protégées contre tout accès non autorisé par des mesures techniques appropriées (authentification sécurisée, mots de passe hashés, connexions chiffrées). Les

sous-traitants impliqués dans les paiements (ex. PayPal) respectent les exigences du RGPD et agissent dans un cadre contractuel sécurisé.

Ces mesures garantissent un haut niveau de protection des droits et libertés des utilisateurs.

Modalités d'information et d'exercice des droits

Les utilisateurs sont informés via :

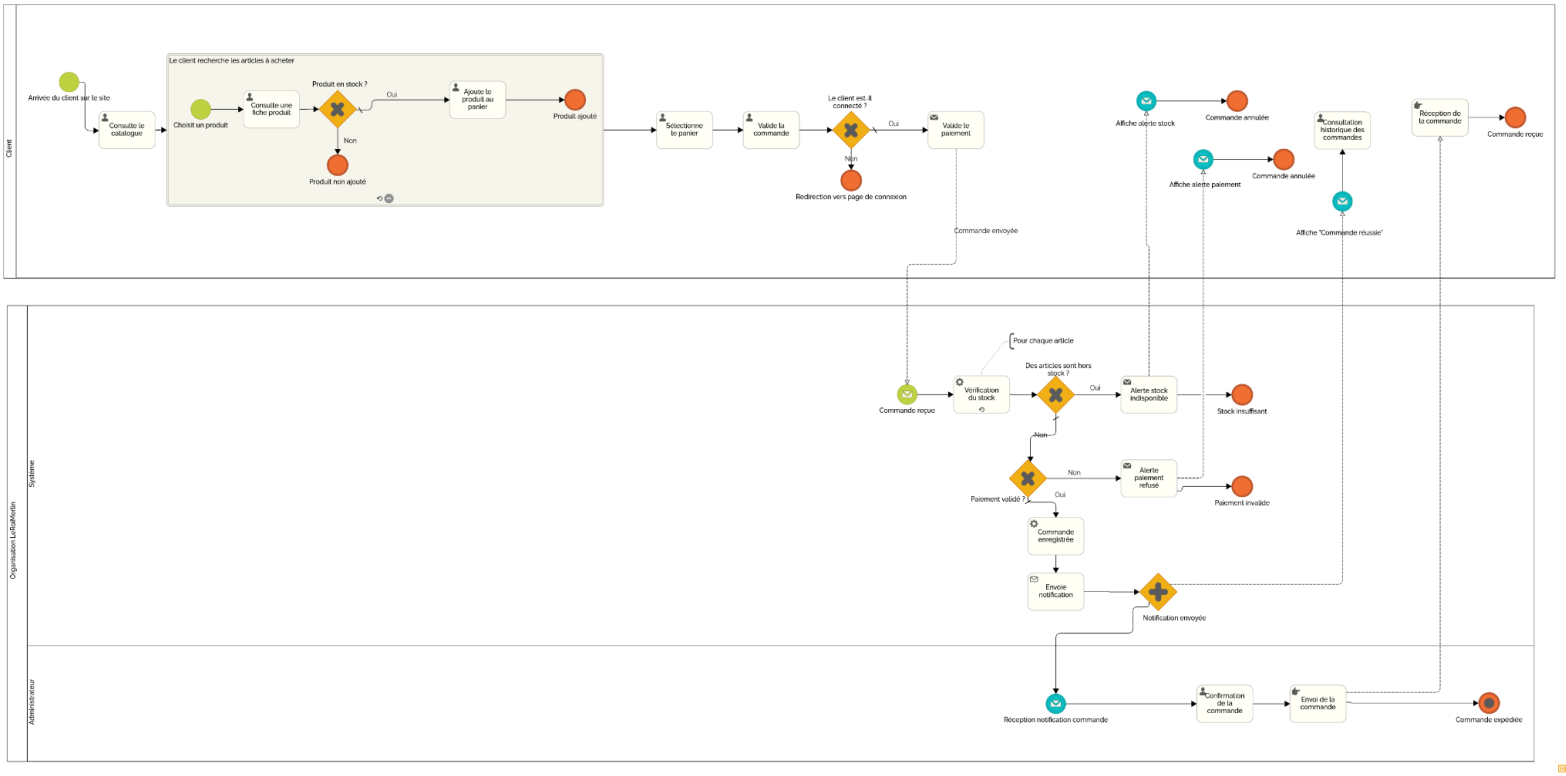
- Une politique de confidentialité accessible en pied de page du site
- Des informations contextuelles lors de la création du compte
- Un bandeau d'information cookies lors de la première visite

Les droits RGPD peuvent être exercés :

- Directement via l'espace client pour l'accès, la rectification et la suppression
- Par email à : contact-rgpd@leroimerlin.fr - Délai de réponse maximum : 30 jours

3. Description des processus et modélisation BPMN

3.1 Processus de commande



Lien de l'image en plus grand :
https://drive.google.com/file/d/1thG6Bh75CXS5D_MnGfjMeGKgw3OqmpiL/view?usp=sharing

Description du processus :
Ce processus débute lorsqu'un utilisateur accède au site LeRoiMerlin et consulte librement le catalogue de produits.Le visiteur sélectionne ensuite les produits souhaités et les ajoute au panier. Il valide son panier pour pouvoir passer commande. L'utilisateur doit posséder un compte client pour passer à l'étape du paiement. *Voir processus de création d'un compte*

Le système vérifie la disponibilité des produits avant toute validation de commande. Si un produit est indisponible, la commande ne peut pas être finalisée.

Après validation du panier, le client procède au paiement via un prestataire sécurisé (PayPal ou carte bancaire). L'enregistrement des données de carte bancaire est proposé de manière optionnelle et soumis à un consentement explicite. En l'absence de consentement, aucune donnée bancaire n'est conservée. Le CVV n'est jamais stocké.

Une fois le paiement validé, la commande est enregistrée et les données de livraison sont utilisées afin d'assurer l'expédition des produits. Le client reçoit une notification de confirmation de commande. L'administrateur est ensuite informé afin de préparer et expédier la commande.

Après réception, le client peut consulter son historique de commandes et, le cas échéant, laisser un avis sur les produits achetés.
Tout au long de la navigation, des cookies techniques sont utilisés pour assurer le bon fonctionnement du site, ainsi que des cookies statistiques limités à l'analyse des produits les plus consultés. Aucun cookie marketing n'est utilisé.

Données personnelles traitées :

- Nom, prénom
- Adresse email
- Mot de passe (hashé)
- Adresse postale
- Numéro de téléphone (le cas échéant)
- Historique des commandes
- Données de paiement (selon consentement explicite)
- Données de navigation via cookies techniques et statistiques

Finalité :

- Identification et authentification des clients
- Gestion des comptes clients
- Exécution du contrat de vente
- Traitement des paiements
- Livraison des produits
- Suivi des commandes et facturation
- Amélioration du service et de l'expérience utilisateur

Mesures RGPD associées :

- Minimisation des données collectées
- Hash sécurisé des mots de passe
- Consentement explicite pour l'enregistrement des données bancaires
- Chiffrement des données sensibles
- Absence de conservation du CVV
- Accès restreint aux données par gestion des rôles
- Droit d'accès, de rectification et de suppression via l'espace client
- Conservation des données limitée et conforme aux obligations légales
- Cookies sécurisés et absence de cookies marketing

3.2 Processus de création et gestion du compte client

Description du processus :
Ce processus débute lorsqu'un utilisateur souhaite créer un compte client afin de pouvoir passer commande sur le site LeRoiMerlin.
L'utilisateur renseigne les données strictement nécessaires à son identification (nom, prénom, adresse email, mot de passe). Le mot de passe est immédiatement hashé avant stockage en base de données.

Une fois le compte créé, le client peut :

- se connecter à son espace personnel,
- modifier ses informations,
- consulter son historique de commandes,
- exercer ses droits RGPD (accès, rectification, suppression).

Données personnelles traitées :

- Nom, prénom
- Adresse email
- Mot de passe (hashé)

Finalité :

- Identification et authentification du client
- Gestion de l'espace personnel

Mesures RGPD associées :

- Minimisation des données collectées
- Hash sécurisé des mots de passe
- Accès restreint aux données
- Droit de suppression du compte

3.3 Processus de gestion des avis clients

Description du processus :
Après livraison d'une commande, le client peut laisser un avis sur les produits achetés.
Seuls les clients ayant effectivement commandé et reçu un produit peuvent publier un avis.

Les avis sont modérés afin de respecter les exigences légales et le Digital Services Act (DSA).

Données personnelles traitées :

- Identité du client
- Contenu de l'avis

Finalité :

- Information des autres clients
- Amélioration du service

Mesures RGPD associées :

- Modération des contenus
- Droit de suppression de l'avis
- Transparence sur l'affichage

3.4 Processus de gestion des cookies

Description du processus :
Le site utilise des cookies techniques nécessaires au fonctionnement du service (session, panier, authentification).
Des cookies statistiques sont utilisés uniquement pour analyser les produits les plus consultés, sans suivi individualisé intrusif.
Aucun cookie marketing n'est utilisé.

Données personnelles traitées :

- Identifiant de session
  Données de navigation anonymisées

Finalité :

- Fonctionnement du site
- Amélioration de l'expérience utilisateur

Mesures RGPD associées :

- Cookies sécurisés
- Information claire à l'utilisateur
- Absence de cookies marketing

4. Description des données et supports

4.1 Données relatives aux comptes clients

Donnée	Description	Finalité	Durée conservation	Sensibilité	Mesures sécurité
Identifiant client	Numéro unique du client	Identification système	3 ans après dernière connexion	Faible	Accès restreint
Nom	Nom de famille	Identification	3 ans après dernière connexion	Moyenne	Chiffrement base
Prénom	Prénom	Identification	3 ans après dernière connexion	Moyenne	Chiffrement base
Email	Adresse email	Connexion, communication	3 ans après dernière connexion	Moyenne	Chiffrement, unicité
Mot de passe	Mot de passe hashé	Authentification	3 ans après dernière connexion	Élevée	Hash SHA-256
Téléphone	Numéro de téléphone	Contact livraison	3 ans après dernière connexion	Moyenne	Optionnel
Date création compte	Date d'inscription	Traçabilité	3 ans après dernière connexion	Faible	-
Dernière connexion	Date dernière connexion	Calcul durée conservation	3 ans après dernière connexion	Faible	-
Statut compte	Actif ou inactif	Gestion compte	3 ans après dernière connexion	Faible	-

4.2 Données relatives aux commandes

Donnée	Description	Finalité	Durée conservation	Sensibilité	Mesures sécurité
Identifiant commande	Numéro unique de commande	Traçabilité	10 ans (obligations comptables)	Faible	-
Référence client	Lien vers le client	Association client-commande	10 ans	Faible	Accès restreint
Date commande	Date et heure de la commande	Facturation, traçabilité	10 ans	Faible	-
Montant total TTC	Prix total payé	Facturation, comptabilité	10 ans	Moyenne	Intégrité données
Statut commande	État (en cours, expédiée, livrée)	Suivi logistique	10 ans	Faible	-
Adresse livraison complète	Adresse postale de livraison	Livraison	1 an après livraison	Élevée	Accès limité
Ville livraison	Ville de livraison	Livraison	1 an après livraison	Moyenne	-
Code postal	Code postal de livraison	Livraison	1 an après livraison	Moyenne	-
Pays livraison	Pays de livraison	Livraison, douanes	1 an après livraison	Faible	-
Mode de paiement	PayPal ou carte bancaire	Traçabilité paiement	10 ans	Faible	-
Référence paiement	Référence transaction externe	Traçabilité, litiges	10 ans	Faible	Fourni par prestataire

4.3 Données relatives aux détails des commandes

Donnée	Description	Finalité	Durée conservation	Sensibilité	Mesures sécurité
Référence commande	Lien vers la commande	Association produits-commande	10 ans	Faible	-
Référence produit	Lien vers le produit	Identification produit acheté	10 ans	Faible	-
Quantité	Nombre d'unités commandées	Facturation, stock	10 ans	Faible	>0
Prix unitaire	Prix au moment de l'achat	Facturation, historique prix	10 ans	Faible	Immutable

4.4 Données de paiement

Donnée	Description	Finalité	Durée conservation	Sensibilité	Mesures sécurité
4 derniers chiffres carte	Identification visuelle carte	Rappel utilisateur	Jusqu'à révocation	Élevée	Chiffrement AES-256
Type de carte	Visa, Mastercard, etc.	Affichage, traitement	Jusqu'à révocation	Moyenne	-
Date expiration	MM/AAAA	Validation paiement	Jusqu'à révocation	Élevée	Chiffrement AES-256
Consentement stockage	Oui/Non	Conformité RGPD	Jusqu'à révocation	Faible	Traçabilité
Date du consentement	Date/heure du consentement	Preuve légale	Jusqu'à révocation	Faible	Immuable
CVV	Code sécurité	Jamais stocké	-	-	-

4.5 Cookies

Type	Finalité	Sensibilité / Commentaires
Cookies techniques	Session, panier, authentification	Faible, nécessaires au fonctionnement du site, ne collectent pas de données personnelles identifiables
Cookies statistiques	Analyse des produits les plus regardés	Faible, données anonymisées, pas de suivi individualisé, conformité RGPD
Cookies marketing	Non utilisés	N/A

5. Analyse des risques cybersécurité

Risque	Menaces	Impacts	Mesures	Gravité
Fuite données bancaires	Piratage BD	Fraude financière	Chiffrement, consentement	Élevée
Accès non autorisé	Vol identifiants	Usurpation	Hash mots de passe, HTTPS, ajouter double authentification, journalisation des connexions sensibles	Moyenne
Perte de données	Défaillance serveur	Interruption service	Sauvegardes	Moyenne
Cookies détournés	Attaque XSS	Vol session	Tokens de session sécurisés, flags HttpOnly et SameSite activés	Faible

6. Mesures de protection des données (RGPD)

Mesure	Modalités	Priorité
Consentement explicite pour le paiement	Case à cocher lors du choix d'enregistrer la carte bancaire	Élevée
Consentement pour cookies statistiques	Pop-up ou bandeau à l'arrivée sur le site	Élevée
Droit d'accès/suppression	Interface client	Élevée
Minimisation des données	Données strictement nécessaires	Moyenne
Durée limitée	Archivage contrôlé	Moyenne

7. Mesures de sécurité des données

Mesure	Modalités / Précisions	Priorité
HTTPS	Connexions chiffrées TLS 1.2 ou supérieur, certificat SSL valide	Élevée
Hash mots de passe	Algorithme sécurisé SHA-256	Élevée
Chiffrement des données CB	Chiffrement AES-256 des données bancaires stockées, CVV jamais conservé	Élevée
Gestion des rôles	Accès aux données limité par profil (client, admin, service logistique)	Moyenne
Sauvegardes	Sauvegardes automatiques quotidiennes, chiffrées, stockées hors site	Moyenne
Journalisation des accès	Enregistrement des accès aux données sensibles pour audit et détection d'incidents	Moyenne
Double authentification	Pour les accès administrateurs ou comptes sensibles	Moyenne

8. Issues à ajouter au dernier sprint

Suite à l'analyse d'impact et après négociation avec le client lors du sprint planning, les priorités suivantes ont été établies :

SPRINT ACTUEL (obligatoire) – Temps estimé : 10h

1. Ajout d'une case de consentement explicite pour l'enregistrement de la carte bancaire (2h) - CRITIQUE
2. Mise en place d'un bouton "Supprimer ma carte enregistrée" (3h) - CRITIQUE
3. Page de gestion des droits RGPD côté client (5h) - ÉLEVÉE

SPRINT DE MAINTENANCE (après lancement)

4. Chiffrement renforcé des données sensibles
5. Journalisation des accès aux données critiques

Le client a validé cette priorisation en privilégiant la conformité légale RGPD pour éviter les risques de sanction.

9. Le Digital Services Act (DSA)

9.1 Résumé du DSA

Le **Digital Services Act (DSA)** est un règlement européen visant à encadrer les services numériques afin de lutter contre les contenus illicites, renforcer la transparence et protéger les utilisateurs.

9.2 Applicabilité à LeRoiMerlin

LeRoiMerlin est :

- un site e-commerce classique,
- sans plateforme de mise en relation,
- sans diffusion massive de contenus tiers.

Le site est faiblement concerné par le DSA, principalement pour :

- la transparence des informations légales,
- la modération des avis clients.

10. Validation de l’analyse d’impact (AIPD)

Au regard des éléments analysés, des finalités poursuivies, des mesures de sécurité mises en œuvre et des risques identifiés, le présent traitement de données personnelles présente des risques maîtrisés pour les droits et libertés des personnes concernées.

Les risques résiduels identifiés sont jugés acceptables au regard des mesures techniques et organisationnelles prévues, notamment le chiffrement des données sensibles, la gestion des accès, le recueil du consentement explicite et la limitation des durées de conservation.

En conséquence, **la présente analyse d’impact relative à la protection des données est jugée conforme et validée**, sous réserve de la mise en œuvre des actions d’amélioration prévues dans le dernier sprint du projet.

11. Conclusion

Cette analyse d’impact montre que le site **LeRoiMerlin** met en œuvre des traitements nécessaires et proportionnés, tout en intégrant des mesures techniques et organisationnelles adaptées.
Les risques identifiés sont maîtrisés grâce aux mécanismes de sécurité et aux mesures RGPD prévues, garantissant la protection des données personnelles des utilisateurs.

Annexe A – Définitions

Cette annexe présente les principales notions juridiques et techniques utilisées dans le cadre de l'analyse d'impact relative à la protection des données (AIPD) du site **LeRoiMerlin**.

AIPD (Analyse d'Impact relative à la Protection des Données)
Analyse visant à identifier, évaluer et réduire les risques qu'un traitement de données personnelles peut faire peser sur les droits et libertés des personnes physiques, conformément à l'article 35 du RGPD.

RGPD (Règlement Général sur la Protection des Données)
Règlement européen (UE) 2016/679 encadrant la collecte, le traitement et la protection des données à caractère personnel au sein de l'Union européenne.

Donnée à caractère personnel
Toute information se rapportant à une personne physique identifiée ou identifiable (ex. nom, adresse email, adresse postale, données de paiement).

Traitement de données
Toute opération effectuée sur des données personnelles, notamment la collecte, l'enregistrement, la consultation, la modification, la conservation ou la suppression.

Responsable de traitement
Entité qui détermine les finalités et les moyens du traitement des données personnelles. Dans ce projet, il s'agit du site e-commerce **LeRoiMerlin**.

Sous-traitant
Entité traitant des données personnelles pour le compte du responsable de traitement, par exemple un prestataire de paiement tel que PayPal.

Consentement explicite
Manifestation de volonté libre, spécifique, éclairée et univoque par laquelle une personne accepte le traitement de ses données personnelles pour une finalité déterminée.

Minimisation des données
Principe du RGPD consistant à ne collecter que les données strictement nécessaires à la réalisation des finalités poursuivies.

Droit d'accès
Droit pour une personne concernée d'obtenir la confirmation que ses données sont traitées et d'en obtenir une copie.

Droit de rectification
Droit permettant à une personne concernée de faire corriger des données inexactes ou incomplètes.

Droit à l’effacement (droit à l’oubli)
Droit permettant à une personne concernée de demander la suppression de ses données personnelles sous certaines conditions.

Cookie
Fichier stocké sur le terminal de l’utilisateur permettant de conserver des informations liées à la navigation (ex. session, panier).

Cookies techniques
Cookies strictement nécessaires au fonctionnement du site et à la fourniture du service demandé par l’utilisateur.

Cookies statistiques
Cookies permettant d’analyser l’usage du site à des fins d’amélioration, sans suivi publicitaire ni profilage marketing.

Hashage
Procédé cryptographique transformant une donnée sensible (ex. mot de passe) en une empreinte irréversible afin de renforcer la sécurité.

Chiffrement
Technique visant à rendre les données illisibles à toute personne non autorisée, notamment pour les données sensibles telles que les informations bancaires.

DSA (Digital Services Act)
Règlement européen encadrant les services numériques, visant à renforcer la transparence et la modération des contenus en ligne

Annexe B – Bibliographie et sources

Les sources suivantes ont été utilisées pour la rédaction de cette analyse d'impact et pour garantir la conformité réglementaire du projet **LeRoiMerlin** :

CNIL – Commission Nationale de l'Informatique et des Libertés
Analyse d'impact relative à la protection des données (AIPD)
https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd

CNIL – Méthode d'écriture du PIA (Privacy Impact Assessment)

Méthode d'écriture de l'analyse d'impact relative à la protection des données (AIPD)

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf

Règlement (UE) 2016/679 – RGPD
Parlement européen et Conseil de l'Union européenne
https://eur-lex.europa.eu/eli/reg/2016/679/oj

CNIL – Principes clés du RGPD
https://www.cnil.fr/fr/comprendre-le-rgpd/les-six-grands-principes-du-rgpd

CNIL – Cookies et traceurs
https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi

Digital Services Act (DSA)
Règlement (UE) 2022/2065
https://digital-strategy.ec.europa.eu/fr/policies/digital-services-act-package

OWASP – Web Application Security
https://owasp.org