ChatGPT

Executive Summary

Un site e-commerce français manipulant des données personnelles et des paiements doit respecter des obligations de sécurité et conformité incontournables. **En priorité**, il s'agit de se conformer au RGPD (notamment l'article 32 exigeant des mesures de protection « **à l'état de l'art** » telles que le chiffrement des données) [1]. Toute **violation de données** doit être notifiée à la CNIL sous 72 heures [2]. Côté paiements, la **norme PCI DSS v4.0** impose de strictes mesures techniques pour les données de cartes bancaires (avec de nouvelles exigences rendues obligatoires au **31 mars 2025** [3]) tandis que la directive européenne **DSP2** impose l'**authentification forte du client** (ex : 3D Secure 2) pour quasiment tous les paiements en ligne [4]. En 2024, Google et Yahoo rendent **SPF, DKIM et DMARC obligatoires** pour les expéditeurs d'e-mails professionnels [5] – un impératif pour garantir la délivrabilité des communications vers les clients. La directive **NIS 2** renforce les exigences cyber (analyse de risques, MFA, politique de gestion des vulnérabilités, etc.) pour les acteurs critiques, ce qui peut inclure les grandes plateformes e-commerce [6]. Enfin, au-delà de la sécurité, les sites marchands devront être **accessibles** à tous : la nouvelle **législation accessibilité** (transposition de la directive UE 2019/882) étend aux sites e-commerce l'obligation de se conformer aux standards WCAG (RGAA v5 en France) d'ici **juin 2025** [7] [8].

Mesures de sécurité et conformité par domaine

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Réseau & transport	**TLS 1.3 et configuration HTTPS robuste** – Criticité : Haute. *Outils :* scanners SSL (Qualys SSL Labs, Mozilla Observatory). *Pièges :* Laisser des versions obsolètes (TLS 1.0/1.1) ou des suites faibles actives. *Indicateur :* Score SSL Labs ≥ A+ (aucune faille connue) [9] [10].	Recommandé (état de l'art)	RGPD art. 32 §1(a) (chiffrement des données) [1] ; ANSSI 2021 (guide HTTPS / HSTS) [10].	Dès maintenant (mise en prod et scans trimestriels).

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Réseau & transport	**HSTS activé, OCSP stapling, HTTP/2+** – Criticité : Moyenne. *Outils :* navigateurs (test du cadenas) et Observatory. *Pièges :* Oublier d'inclure les sous-domaines ou d'inscrire le domaine en preload HSTS (liste navigateur). *Indicateur :* Présence de l'en-tête Strict-Transport-Security max-age ≥ 6 mois [10].	Recommandé	Politique HSTS (RFC 6797) – exigence navigateurs modernes [10].	Dès mise en service (vérifier à chaque déploiement).
Réseau & transport	**Protection DDoS et pare-feu applicatif (WAF)** – Criticité : Haute. *Outils :* services Anti-DDoS (Cloudflare, Akamai) ; WAF open-source (ModSecurity/OWASP CRS) ou cloud (AWS WAF, F5, Cloudflare). *Pièges :* Faux positifs du WAF bloquant des clients légitimes ; coûts et limites des solutions DDoS si sous-dimensionnées. *Indicateur :* Score sécurité backend (ex: OWASP ASVS 14.4) et tests de résistance aux attaques volumétriques.	Fortement recommandé	CNIL 2024 (distinction Anti-DDoS vs CDN) [11] ; RGPD art. 32 (intégrité, dispo) [12].	En continu (supervision 24/7 ; tests de charge annuels).

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Réseau & transport	**Segmentation réseau & filtrage** – Criticité : Haute. *Outils :* pare-feux (iptables, Cisco ASA) isolant les composants (frontaux web, bases de données) ; VLAN séparés. *Pièges :* Ports ouverts inutilement exposés ; absence de détection sur le trafic interne. *Indicateur :* Scan de ports externe (doit être minimal) et interne ; audit de config réseau.	Obligatoire (PCI DSS)	PCI DSS Req. 1 (firewall, segmentation de la zone carte) [13] ; ANSSI 40 mesures.	Contrôle permanent (revue règles fw trimestrielle).
DNS & e-mail	**Authentification des e-mails (SPF, DKIM, DMARC)** – Criticité : Haute. *Outils :* générateurs SPF (DMARCAdvisor), clés DKIM (OpenDKIM), analyse rapports DMARC (DMARCian). *Pièges :* SPF trop permissif (include ?all) ; clé DKIM mal déployée ; politique DMARC non restrictive (p=none) ne détectant pas l'usurpation. *Indicateur :* DMARC aligné et politiques publiées (analysées via outils en ligne).	Obligatoire (livraison mail)	Google / Yahoo (dès fév. 2024 exigent DMARC + SPF/DKIM alignés) [5] .	Immédiat (sous peine de rejet mails dès 2024).

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
DNS & e-mail	**DNSSEC déployé & enregistrements CAA** – Criticité : Moyenne. *Outils :* DNS gérant DNSSEC (AFNIC, Cloudflare) ; test via DNSViz. *Pièges :* Mauvaise rotation des clés DNSSEC (risque d'expiration) ; absence d'enregistrement CAA (permettant à n'importe quelle AC d'émettre un certificat frauduleux). *Indicateur :* Domaine signé DNSSEC valide (aucune erreur) ; enregistrement CAA autorisant uniquement l'AC choisie.	Recommandé	Recommandé par ANSSI pour l'intégrité DNS (Good practice) ; CAB Forum Baseline (CAA).	Dès que possible (avant mise en prod du site).

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Application & API	**En-têtes HTTP de sécurité** (CSP, X-Frame-Options / `frame-ancestors`, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, COOP/COEP/CORP) – Criticité : Moyenne. *Outils :* scanners (Mozilla Observatory, OWASP SecureHeaders) pour vérifier les headers. *Pièges :* CSP trop permissive (`unsafe-inline`), rendant la protection inefficace ; oublier `frame-ancestors` (successeur de X-Frame-Options) contre le clickjacking. *Indicateur :* Score Observatory ≥ B ; absence d'avertissements sur securityheaders.com.	Recommandé	Guide ANSSI 2021 (63 recommandations côté navigateur) [14] ; OWASP ASVS 14.5 (Secure headers).	Vérifier à chaque déploiement (headers constants).

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Application & API	**Cookies sécurisés** (`Secure`, `HttpOnly`, `SameSite`, préfixe `__Host-`) – Criticité : Haute. *Outils :* tests via un navigateur en mode dev (lecture des drapeaux sur les cookies) ; outils comme Hardenize. *Pièges :* Oublier `HttpOnly` (exposant le cookie aux scripts XSS) ; SameSite mal paramétré rompant certaines intégrations tierces (ex : paiement externalisé). *Indicateur :* Aucun cookie de session sans `Secure` ni `HttpOnly` ; usage de `SameSite=Lax` par défaut.	Recommandé	RGPD art. 32 (intégrité sessions) ; OWASP Cheat Sheet (Cookie Safety).	Dès la mise en prod ; contrôles réguliers (scans mensuels).

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Application & API	**Fichier sécurité .txt** (`/.well-known/security.txt`) – Criticité : Bas. *Outils :* générateur de fichier security.txt (template RFC 9116). *Pièges :* Informations obsolètes (contact plus valide) ; oublier de le mettre à jour après un changement d'équipe sécurité. *Indicateur :* Fichier accessible via `https://site/.well-known/security.txt` fournissant un contact de vulnérabilité.	Recommandé	RFC 9116 (2022) – standard de divulgation coordonnée.	À publier dès le lancement du site ; MAJ à chaque changement de contact.

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Application & API	**Authentification renforcée (MFA & MDP sécurisés)** – Criticité : Haute. *Outils :* Gestionnaires d'authentification 2FA (PrivacyIDEA, Duo, Microsoft/ Google Auth) ; vérificateurs de mots de passe compromis (HaveIBeenPwned API). *Pièges :* Se limiter au seul couple login+password (vulnérable au **credential stuffing** en 2024) ; politique MDP trop complexe menant à des mots de passe faibles (utilisateurs frustrés). *Indicateur :* MFA activé pour les comptes admin/ sensibles ; stockage des MDP par fonction de hachage salé (bcrypt/ Argon2) ; taux de réussite d'attaques par force brute ≈ 0.	Obligatoire (hauts risques)	RGPD art. 32 (auth. robuste si données bancaires) ; CNIL 2025 (MFA requis si risques élevés, ex. données bancaires) [15] ; ANSSI 2022 (référentiel MDP).	Dès que possible (MFA prod 2024) ; révision politique MDP annuelle.

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Application & API	**Journalisation & détection d'intrusion** – Criticité : Haute. *Outils :* SIEM (ELK, Splunk) agrégeant les logs ; sondes IDS (Suricata, Wazuh) et EDR. *Pièges :* Collecter des volumes de logs énormes sans les exploiter (« bruit » qui masque les incidents réels) ; oublier de journaliser les échecs d'accès ou les appels d'API. *Indicateur :* Conservation des journaux ≥ 6 mois [16] sur une plateforme séparée ("log sink") ; alertes en temps réel sur activités suspectes (ex: connexion admin hors heures ouvrées).	Obligatoire (état de l'art)	RGPD art. 32 §1(b) (intégrité, traçabilité) ; CNIL reco. journalisation (2021) [16] ; PCI DSS Req. 10 (logs) et 11.4 (IDS).	En continu (supervision quotidienne ; audit des logs mensuel).

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Application & API	**Chiffrement des données *au repos*** (stockage chiffré) & **gestion des clés** – Criticité : Haute. *Outils :* chiffrement disque/partition (BitLocker, LUKS) ; base de données chiffrée (TDE Oracle/ SQL Server) ; coffres-forts à clés (HSM, AWS KMS, HashiCorp Vault). *Pièges :* Stocker la clé de déchiffrement sur le même serveur que les données chiffrées (rend le chiffrement inutile en cas de compromission) ; négliger de renouveler régulièrement les clés. *Indicateur :* Données sensibles (ex : mots de passe, numéros de carte chiffrés ou hachés) tant en base qu'en sauvegardes ; journal des accès aux clés sans anomalie.	Obligatoire (risques élevés)	RGPD art. 32 §1(a) (chiffrement des données pers.) [1] ; CNIL 2025 (chiffrer transit & repos) [9] ; PCI DSS Req. 3 (chiffrement PAN).	Dès la conception (données clients chiffrées avant prod) ; rotation clés annuelle.

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Application & API	**Cycle DevSecOps & Supply chain** – Intégration de la sécurité dans le développement (SAST, DAST, SCA) + maîtrise des dépendances et builds (signature CI/CD, SBOM). Criticité : Moyenne. *Outils :* analyse statique (SonarQube + plugin sécurité, Semgrep) ; analyse dynamique (OWASP ZAP, Burp) ; SCA (OWASP Dependency-Check, Snyk) ; signature de code (Cosign, Sigstore) ; SBOM (CycloneDX, Syft). *Pièges :* Ignorer les alertes de vulnérabilités connues dans les libs ; pipelines CI/CD non protégés (risque de compromission de supply chain type SolarWinds). *Indicateur :* **SBOM** à jour listant 100% des composants tiers ; rapports de scan **OWASP Top 10** sans faille critique avant mise en prod ; packages déployés signés et vérifiés.	Recommandé (state of the art)	NIS 2, art 21 §2(e)-(f) (sécurité dev + gestion vuln.) [17] ; CNIL 2025 (tests de sécu réguliers, mises à jour composants) [18] ; OWASP SAMM.	Intégré CI/CD (scans à chaque build) ; audit code annuel par tiers.

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Paiement	**Conformité PCI DSS v4.0** (Protection des données de carte) – Criticité : Haute. *Outils :* référent PCI interne ou QSA ; scanners ASV trimestriels (Qualys) ; tokenisation PAN (via PSP). *Pièges :* Stocker localement des numéros de carte en clair (strictement interdit) ; oublier les tests de pénétration annuels obligatoires. *Indicateur :* Attestation de conformité PCI-DSS valide (SAQ D ou ROC par auditeur) ; zéro stockage de données sensibles non justifié.	Obligatoire (si CB)	Standard PCI DSS v4.0 (mars 2022) – 51 nouvelles exigences effectives 31/03/2025 [3] .	Transition v3.2.1→v4.0 jusqu'au 31 mars 2024 ; exigences v4.0 finales d'ici 31 mars 2025.

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Paiement	**Authentification forte du client (SCA)** – Criticité : Haute. *Outils :* module 3D Secure 2 via la banque ou PSP ; authentification bancaire (ex : API d'Open Banking pour virement). *Pièges :* Friction utilisateur accrue si SCA mal implémentée (abandon panier) ; croire à tort que de petites transactions seraient exemptées (seules < 30 € le sont souvent, et selon taux de fraude). *Indicateur :* 100 % des paiements électroniques soumis à 3D Secure 2 ou équivalent (sauf exemptions réglementaires) ; taux de fraude post-SCA en baisse.	Obligatoire	Directive DSP2 2015/2366 (transposée ord. 2017) – **authentification forte requise** pour paiements en ligne [4] (appliquée en France depuis 05/2021).	Immédiat (déjà en vigueur depuis 2021).

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Paiement	**Conformité RGPD & bancaire des wallets / open-banking** – Criticité : Haute. *Outils :* recours à des prestataires agréés (PSP, API bancaires conformes) évitant de manipuler soi-même des données sensibles ; vérifications contractuelles (DPA, clauses sécurité). *Pièges :* Collecter des IBAN ou données bancaires sans base légale (le paiement doit être opéré par un prestataire habilité DSP2) ; ne pas vérifier que le prestataire applique lui-même PCI DSS et la réglementation financière. *Indicateur :* Existence de contrats de sous-traitance (article 28 RGPD) avec chaque fournisseur de paiement ; documentation d'architecture prouvant qu'aucune donnée bancaire complète n'est stockée sur le site marchand.	Obligatoire	Code monétaire et financier (DSP2) ; RGPD art. 28 (sous-traitants sécurisés) [19] [20] .	Dès la conception (choisir un PSP conforme) ; audits annuels des partenaires critiques.

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Gouvernance & conformité	**Analyses de risque & politique SSI** – Criticité : Haute. *Outils :* méthode EBIOS RM ou ISO 27005 pour formaliser les risques ; élaboration d'une PSSI (Politique de Sécu du SI) et chartes internes. *Pièges :* Négliger certains scénarios (ex : menace interne) ; documenter puis ne pas appliquer (PSSI purement théorique). *Indicateur :* Registre des risques à jour (réévalué au moins annuellement) ; politique de sécurité validée par la direction et diffusée aux équipes (avec approbation formelle).	Obligatoire	RGPD art. 32 §1 (mesures proportionnées aux risques) [21] ; Directive NIS 2 art. 21 §2(a) (analyse des risques) [22] .	Analyse à initier en phase de design ; mises à jour annuelles ou à chaque changement majeur.

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Gouvernance & conformité	**Gestion des incidents & notification** – Criticité : Haute. *Outils :* plan de réponse cyber (playbook) incluant formulaires de notification CNIL ; contrat avec un CSIRT externe au besoin. *Pièges :* Découvrir trop tard une fuite faute de surveillance ; omettre de notifier la CNIL dans les 72h ou de communiquer aux clients si nécessaire (risque de sanction aggravé). *Indicateur :* Procédure interne de gestion des failles existante (testée via exercices) ; registre des violations tenu (même pour incidents mineurs) [23] .	Obligatoire	RGPD art. 33 (notification CNIL < 72h) [2] & 34 (information des personnes) ; NIS 2 (incidents significatifs : alerte 24h).	Procédures en place dès prod ; tests plan (PCN/ PRA) 1×/an ; notification CNIL sous 3 jours si incident.

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Gouvernance & conformité	**Contrats & sous-traitants sécurisés** – Criticité : Haute. *Outils :* clauses contractuelles RGPD avec chaque prestataire (hébergement, paiement, emailing) ; évaluation de leurs certifications (ISO 27001, SecNumCloud, PCI DSS…). *Pièges :* Ne pas formaliser de DPA (Data Processing Agreement) ; choisir un fournisseur non conforme (ex: hébergeur hors UE sans garanties, entraînant transfert illégal). *Indicateur :* Dossiers d'homologation ou audits tierce partie disponibles pour les principaux prestataires ; clauses de sécurité et notification d'incident insérées aux contrats.	Obligatoire	RGPD art. 28 (sous-traitance) : choisir des prestataires offrant des garanties de sécurité [24] [20] ; NIS 2 §2(d) (sécurité supply chain) [17] .	Avant tout engagement de prestataire ; revue annuelle des contrats critiques.

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Gouvernance & conformité	**Formation et sensibilisation sécurité** – Criticité : Moyenne. *Outils :* modules e-learning (ANSSI SecNumacadémie) ; campagnes de phishing test (GoPhish) ; ateliers en présentiel. *Pièges :* Se limiter à une formation à l'embauche puis rien ; négliger la formation des développeurs sur les erreurs courantes (ex: injections, XSS). *Indicateur :* % d'employés formés cette année ≥ 95 % ; quiz internes post-formation validés ; diminution des incidents liés à l'erreur humaine.	Obligatoire (RGPD)	RGPD art. 32 (mesures orga. = former le personnel) [25] ; CNIL avr. 2025 (sensibilisation régulière) [26] ; NIS 2 §2(g) (hygiène cyber, formation) [27] .	Programme de formation initiale + rappels au moins 1×/an (avec mise à jour continue des contenus).

Domaine	Mesure ou protocole (avec criticité, outils, pièges, indicateurs)	Statut	Texte / norme de référence	Deadline / Fréquence
Gouvernance & conformité	**Plans de continuité et sauvegardes** – Criticité : Haute. *Outils :* backups chiffrés hors-site (fréquence quotidienne ou incrémentielle) ; plan de reprise d'activité (PRA) documenté et outillé. *Pièges :* Tester la restauration trop tard – découvrir que les sauvegardes sont corrompues ou incomplètes en plein incident ; oublier de couvrir tous les composants critiques (DB, fichiers, configs). *Indicateur :* RPO/RTO définis et respectés en test ; résultats d'exercices PRA démontrant une reprise < objectif (ex: service rétabli < 4h suite sinistre).	Obligatoire (disponibilité)	RGPD art. 32 §1(c) (disponibilité : restauration après incident) [12] ; NIS 2 §2(c) (plans de continuité) [28] .	Backups : au moins quotidiens (avec tests trimestriels de restauration) ; PRA : test complet 1×/an.

Accessibilité & obligations connexes

- **Conformité Accessibilité Web (RGAA v5 / WCAG 2.1)** – La directive UE 2016/2102 (sites publics) élargie par l'**European Accessibility Act** 2019/882 (transposé par décret n°2023-931) rendra **obligatoire d'ici juin 2025** le respect des standards d'accessibilité numérique pour les sites e-commerce et services de paiement [7] [8] . Criticité : Moyenne (conformité légale, risque réputation). *Outils :* Validateurs RGAA (AccessMonitor) ; lecteurs d'écran (NVDA) pour tests. *Pièges :* Se contenter d'une déclaration d'accessibilité générique sans corriger les problèmes réels ; négliger la compatibilité mobile (aussi requise). *Indicateur :* Taux de conformité RGAA v5 $\geq$ expected (ex: 90+ %) ; audit indépendant OK.
- **Double clic & confirmation de commande** – En vente en ligne, le **processus de consentement** doit comporter deux étapes : validation de la commande puis confirmation explicite après récapitulatif, avec un bouton indiquant clairement l'« obligation de paiement » [29] . En l'absence de ce **« double clic »**, le contrat électronique est nul. Criticité : Haute (condition de validité des ventes). *Références :* C. consommation art. L221-14 et C. civil art. 1127-2 [29] .
- **Archivage des contrats électroniques** – Le Code de la consommation oblige à **conserver le contrat** lorsque la vente porte sur $\geq$ 120 € ; le e-commerçant doit archiver l'écrit pendant **10 ans** et le tenir à disposition du client sur demande [30] . Criticité : Moyenne (sécurité juridique). *À*

faire : mettre en place un stockage durable et sécurisé des confirmations de commande (PDF horodatés, etc.).

- **Mentions légales & vie privée** – Afficher sur le site les informations légales obligatoires (identité de l'éditeur, contacts) et une **politique de confidentialité conforme RGPD**. Criticité : Haute (obligation légale LCEN, RGPD art. 13/14). Veiller à fournir un moyen simple d'exercer les droits RGPD (formulaire de contact ou adresse DPO).

Checklist de sécurité & conformité (projet e-commerce) :

- [ ] **Chiffrement HTTPS à jour** (TLS 1.2/1.3 activé, HSTS préchargé, config A+ sur SSL Labs).
- [ ] **Headers HTTP de sécurité déployés** (CSP, XSS-Protection[1], X-Frame-Options[1]/frame-ancestors, etc.).
- [ ] **Cookies sécurisés** (`Secure`, `HttpOnly`, `SameSite`, préfixes `__Host-` / `__Secure-`).
- [ ] **Anti-DDoS et WAF en place** (protection contre floods, injections SQL/XSS, bots).
- [ ] **Surveillance & journaux** centralisés (logs conservés ≥ 6 mois, SIEM avec alertes en temps réel).
- [ ] **Gestion identités renforcée** (MFA activé sur comptes admins/utilisateurs sensibles ; MDP robustes stockés en hash salé).
- [ ] **Chiffrement des données au repos** (bases clients chiffrées, backups sécurisés hors-site) + **coffre de clés**.
- [ ] **Processus DevSecOps intégré** (analyses SAST/DAST/SCA à chaque build, correctifs appliqués avant prod).
- [ ] **Tests d'intrusion réguliers** (au moins 1×/an par un tiers) et scans de vulnérabilités trimestriels.
- [ ] **Conformité PCI DSS** (segmentation du PAN, scans ASV trimestriels, audits annuels, aucune donnée carte en clair).
- [ ] **Authentification forte des paiements** (3D Secure 2 implémenté via votre PSP pour toutes les transactions).
- [ ] **Procédures incidents** (plan de réponse, équipe contactable 24/7, notification CNIL prête sous 72h).
- [ ] **Contrats & RGPD** (registre des traitements, analyse de risques/DPIA, sous-traitants avec clauses de sécurité, DPO désigné si applicable).
- [ ] **Formation sensibilisation** du personnel (campagnes annuelles, tests de phishing, refresh dev secure coding).
- [ ] **Accessibilité web conforme** (audit RGAA v5, corrections en cours pour échéance 2025, déclaration d'accessibilité en ligne).
- [ ] **Exigences e-commerce légales** (double clic de confirmation, archivage contrats ≥ 120 € pour 10 ans, mentions légales & CGV/CGU visibles).

<small>[1] XSS-Protection : entête maintenant obsolète, remplacé par Content Security Policy (CSP). </small>

Sources : RGPD (2016/679) [1] [2] ; CNIL (recommandations 2021–2025) [15] [9] ; Directive NIS 2 (UE 2022/2555) [6] ; PCI DSS v4.0 [3] ; Google & Yahoo mail requirements [5] ; Code de la consommation (articles L221-14 [29], L213-1 [30] …).

---

[1] [12] Article 32 : Sécurité du traitement - GDPR.expert
https://www.gdpr-expert.eu/article.html?id=32

2 23 Article 33 - Notification à l'autorité de contrôle d'une violation de données à caractère personnel
https://www.alowa.fr/articles-rgpd/article-33-notification-a-lautorite-de-controle-dune-violation-de-donnees-a-caractere-personnel

3 13 Now is the Time for Organizations to Adopt the Future-Dated Requirements of PCI DSS v4.x
https://blog.pcisecuritystandards.org/now-is-the-time-for-organizations-to-adopt-the-future-dated-requirements-of-pci-dss-v4-x

4 Paiements en ligne : l'authentification forte DSP2 pour sécuriser votre site e-commerce est désormais obligatoire - francenum.gouv.fr
https://www.francenum.gouv.fr/guides-et-conseils/developpement-commercial/solutions-de-paiement/paiements-en-ligne

5 The Gmail, Microsoft, and Yahoo DMARC requirements on the domains platform : OpenSRS Customer Support
https://support.opensrs.com/support/solutions/articles/201000063028-the-gmail-microsoft-and-yahoo-dmarc-requirements-on-the-domains-platform

6 17 22 27 28 NIS 2 Directive, Article 21: Cybersecurity risk-management measures
https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html

7 8 France – a pioneer in accessibility legislation
https://www.datenschutz-notizen.de/france-a-pioneer-in-accessibility-legislation-0552355/

9 18 CNIL : Nouvelles recommandations pour les applications mobiles | News | Graces.community
https://www.graces.community/post/cnil-nouvelles-recommandations-applications-mobiles-1

10 ssi.gouv.fr
https://www.ssi.gouv.fr/uploads/2013/05/anssi-guide-recommandations_mise_en_oeuvre_site_web_maitriser_standards_securite_cote_navigateur-v2.0.pdf

11 Informatique en nuage (cloud) : la CNIL publie deux fiches pratiques sur le chiffrement et la sécurité des données | CNIL
https://www.cnil.fr/fr/informatique-en-nuage-cloud-la-cnil-publie-deux-fiches-pratiques-sur-le-chiffrement-et-la-securite

14 Guide ANSSI : focus sur les mécanismes de sécurité des navigateurs | IT-Connect
https://www.it-connect.fr/guide-anssi-focus-sur-les-mecanismes-de-securite-des-navigateurs/

15 16 19 20 21 24 25 26 La CNIL donne ses consignes pour renforcer la sécurité des grandes bases de données | CNIL
https://www.cnil.fr/fr/consignes-pour-renforcer-la-securite-des-grandes-bases-de-donnees

29 Que faut-il savoir avant de souscrire un contrat de communications électroniques ? | Arcep
https://www.arcep.fr/mes-demarches-et-services/consommateurs/fiches-pratiques/la-souscription-a-un-contrat-de-communications-electroniques.html

30 Chapitre III : Conservation des contrats conclus par voie électronique (Article L213-1) - Légifrance
https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006069565/LEGISCTA000032221221/