SARL **ITALIC** • 8 BIS RUE ABEL • 75012 PARIS
TEL +33 (0)1 48 44 46 35 • **MAIL** HELLO@ITALIC.FR • **NEWS** WWW.ITALIC.FR
RCS B PARIS 508228772 • **NAF** 6201Z • **TVA** FR73508228772 • **CAP.** 3 550 €

RÉFÉRENTIEL ITALIC DE CONFORMITÉ, SÉCURITÉ ET QUALITÉ NUMÉRIQUE

Mise à jour du 22 septembre 2025

Conforme à la doctrine CNIL 2025, et en accord avec le PCI DSS v4.0

Préambule

Le présent Référentiel ITALIC de conformité, sécurité et qualité numérique définit les engagements pris par ITALIC dans l'exécution de ses prestations digitales.

Il regroupe et harmonise l'ensemble des règles applicables à nos activités, couvrant :

- **Conformité réglementaire :** respect du Règlement Général sur la Protection des Données (RGPD), de la Loi Informatique et Libertés, des lignes directrices de la CNIL, et des référentiels d'accessibilité et d'éco-conception publiés par l'État français.
- **Sécurité des données :** engagements en matière de confidentialité, intégrité et disponibilité, y compris la conformité au standard PCI DSS pour les solutions de paiement.
- **Qualité logicielle :** respect des bonnes pratiques de développement, correction des anomalies, processus d'audit et d'amélioration continue.
- **Résilience et continuité d'activité :** sauvegardes, plan de reprise d'activité (PRA), engagements de disponibilité (SLA).
- **Assurance et responsabilités :** garanties professionnelles d'ITALIC, périmètre des obligations de moyens et de résultat, répartition des responsabilités avec les Clients et prestataires tiers.

Table des matières

1. Préambule : Qu’est-ce qu’une donnée personnelle ?

Est considérée comme donnée personnelle toute information se rapportant à une personne physique identifiée ou identifiable.

Une personne peut être identifiée :

- **directement** : nom, prénom, etc.
- **indirectement** : numéro client, numéro de téléphone, donnée biométrique, éléments relatifs à son identité physique, génétique, psychique, culturelle, sociale, voix, image, etc.

L’identification peut être réalisée :

- à partir d’une seule donnée (ex. : numéro de sécurité sociale, ADN),
- à partir du croisement de plusieurs données (ex. : femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militante dans telle association).

Chaque traitement doit avoir un **objectif précis et légitime**. La collecte « au cas où » est interdite.

2. Respect du RGPD dans le cadre de nos opérations générales

2.1. Cadre général

Nos contacts incluent prospects, clients, fournisseurs et utilisateurs de nos services (sites web, plateformes de gestion, mailing-lists).

Conformément à l’article 30 du RGPD, ITALIC tient un registre des traitements précisant :

- **Finalités et bases légales** :

    - Contrat (exécution des prestations),
    - Obligation légale (facturation, comptabilité, droit du travail),
    - Consentement (prospection, newsletters, cookies),
    - Intérêt légitime (sécurité, prévention de la fraude).

- **Catégories de données** : identité, coordonnées, données RH, données contractuelles, etc.
- **Destinataires** : services internes (commercial, RH, informatique), prestataires, hébergeurs, partenaires.
- **Responsable du traitement** : ITALIC, représentée par son gérant **Germain Guglielmetti**.
- **Délégué à la protection des données (DPO)** : Germain Guglielmetti – contact : germain@italic.fr.
- **Durées de conservation** adaptées à chaque finalité (voir §3.5).
- **Mesures de sécurité techniques et organisationnelles** documentées.
- **Droit de réclamation** : toute personne concernée peut saisir la CNIL (www.cnil.fr).

Les personnes concernées peuvent exercer leurs droits par courrier électronique ou postal adressé au DPO.

2.2. Protection des données dès la conception et par défaut

ITALIC intègre la protection des données dans ses outils, produits et services dès leur conception. Par défaut, seules les données strictement nécessaires sont traitées, en limitant leur volume, durée de conservation et nombre d'accès.

2.3. Prospects, clients, fournisseurs

Données collectées : identité et coordonnées professionnelles, pour l'envoi de documents commerciaux et réglementaires.
Durées de conservation :

- Prospects : 3 ans après le dernier contact,
- Clients : durée du contrat + 5 ans,
- Facturation/comptabilité : 10 ans.

2.4. Employés, stagiaires, apprentis, associés

Données collectées : données RH et sociales nécessaires au respect des obligations légales et comptables.
Durées de conservation :

- Dossier du personnel : 5 ans après départ,
- Bulletins de paie : 5 ans,
- Données relatives aux accidents du travail : 5 ans (40 ans pour expositions spécifiques).

3. Respect du RGPD dans le cadre des prestations clients

3.1. Définitions

Dans l'exécution de ses prestations, ITALIC peut traiter des données personnelles appartenant au Client (responsable du traitement). ITALIC agit en qualité de **sous-traitant** au sens de l'article 28 du RGPD.

3.2. Engagements

ITALIC s'engage à :

- Traiter les données uniquement sur instructions documentées du Client,

- Assurer sécurité, intégrité et confidentialité des données,
- Mettre en œuvre des mesures organisationnelles et techniques adaptées,
- Limiter l'accès aux seules personnes habilitées,
- Ne pas communiquer de données à des tiers non autorisés,
- Répercuter ses obligations de confidentialité à ses propres sous-traitants,
- Notifier toute violation de données au Client sans délai et l'assister pour la déclaration CNIL sous 72h,
- Restituer ou supprimer les données à la fin du contrat.

3.3. Sous-traitants

ITALIC peut recourir à des sous-traitants tiers, en garantissant qu'ils respectent les mêmes obligations. La liste actualisée des sous-traitants est disponible sur demande.

3.4. Exercice des droits

Les personnes concernées disposent des droits d'accès, rectification, effacement, limitation, portabilité et opposition.

- L'exercice est gratuit pour la personne concernée (sauf abus).
- ITALIC assiste le Client dans le traitement de ces demandes.
- Si ITALIC agit directement à la place du Client, ce service pourra être facturé **uniquement à la demande expresse du Client**.

3.5. Grille pratique RGPD

Type de donnée	Base légale	Durée de conservation	Destinataires

Prospects (identité, email, téléphone)	Consentement ou intérêt légitime	3 ans après dernier contact	Service commercial, marketing
Clients (identité, coordonnées, facturation)	Contrat / obligation légale	Durée du contrat + 5 ans	Service commercial, comptabilité, direction
Factures et pièces comptables	Obligation légale (Code de commerce)	10 ans	Comptabilité, administration fiscale
Logs techniques (IP, connexions)	Intérêt légitime (sécurité)	12 mois	Service informatique, hébergeur
Données RH (dossier salarié, contrats, paie)	Contrat de travail / obligation légale	5 ans après départ salarié (40 ans pour expositions spécifiques)	RH, comptabilité, organismes sociaux
Données de formation / stagiaires	Contrat / obligation légale	5 ans après fin de stage/apprentissage	RH, organismes sociaux, tuteur
Données fournisseurs (contrats, coordonnées)	Contrat / obligation légale	Durée du contrat + 5 ans	Comptabilité, direction

Données marketing (tracking, préférences)	Consentement	Jusqu'au retrait du consentement ou 3 ans après dernier contact	Service marketing, outils tiers (si consentement)

4. Acceptation des termes de la Charte

4.1. Clients

La signature d'un bon de commande comportant un lien vers la présente Charte emporte acceptation de celle-ci.

4.2. Employés

La clause de confidentialité figurant dans le contrat de travail s'applique aux données traitées. Elle perdure après la rupture du contrat.
Tout manquement expose le collaborateur à des sanctions disciplinaires ou pénales.
ITALIC organise des **actions de sensibilisation et formations régulières** à la protection des données.

5. Cookies et traceurs

Les sites développés et exploités par ITALIC :

- intègrent une solution de gestion des consentements (CMP) conforme aux lignes directrices de la CNIL,

- n'installent aucun cookie non essentiel sans consentement préalable de l'utilisateur.

6. Analyses d’impact (AIPD/DPIA)

ITALIC informe le Client si un traitement nécessite une analyse d’impact (profilage, données sensibles, surveillance à grande échelle) et l’assiste dans cette démarche.

7. Sécurité – Conformité PCI DSS

7.1. Objet

Cette section définit la répartition des responsabilités liées à la conformité PCI DSS (Payment Card Industry Data Security Standard). Deux cas sont prévus :

- **Cas A** : ITALIC prestataire de développement,
- **Cas B** : ITALIC éditeur de plateforme sous licence.

7.2. Cas A – ITALIC prestataire de développement

ITALIC :

- Développe selon les bonnes pratiques de sécurité (OWASP, PCI DSS),
- Intègre uniquement des prestataires certifiés PCI DSS (Stripe, Stancer, Qonto, PayPal…),
- Livre un code sans stockage de données bancaires,
- Fournit des correctifs de sécurité uniquement dans le cadre d’un **contrat de maintenance**.

Client :

- Met en place une infrastructure conforme PCI DSS,

- Choisit et contracte avec le prestataire de paiement,
- Réalise les audits PCI DSS requis (SAQ, QSA),
- Assure supervision et gestion des incidents.

7.3. Cas B – ITALIC éditeur de plateforme

ITALIC (éditeur) :

- Conçoit le logiciel sans stockage de données de cartes,
- Intègre uniquement des PSP certifiés PCI DSS,
- Publie les correctifs et évolutions de sécurité (sous réserve de souscription à un forfait de suivi),
- Fournit documentation et support,
- Assiste en cas d'incident logiciel.

Client (licencié) :

- Exploite la plateforme sur une infrastructure sécurisée,
- Configure correctement les modules de paiement,
- Définit une politique interne de sécurité et forme son personnel,
- Réalise ses audits PCI DSS,
- Supervise les accès et notifie ITALIC en cas d'incident.

7.4. Tableau de répartition

Domaine	Cas A – ITALIC prestataire	Cas B – ITALIC éditeur
Développement sécurisé	✅ ITALIC	✅ ITALIC
Intégration PSP certifiés PCI DSS	✅ ITALIC	✅ ITALIC
Stockage de données bancaires	❌ (jamais)	❌ (jamais)
Correctifs de sécurité logiciel	✅ ITALIC (si contrat maintenance)	✅ ITALIC
Hébergement / infrastructure réseau	✅ Client (ou ITALIC si option hébergement)	✅ Client (ou ITALIC si option hébergement)
Gestion des accès administrateurs	✅ Client	✅ ITALIC
Politique de sécurité interne	✅ Client	✅ Client
Sensibilisation du personnel	✅ Client	✅ Client
Audits PCI DSS	✅ Client	✅ Client

Support en cas d'incident logiciel	❌	✅ ITALIC

7.5. Limitation de responsabilité

ITALIC n'est pas responsable de la non-conformité PCI DSS résultant :

- d'une configuration inadaptée par le Client,
- de l'utilisation d'un prestataire non certifié PCI DSS,
- de manquements organisationnels ou techniques imputables au Client.

8. Hébergement des sites et applications

8.1. Hébergement

ITALIC n'est pas hébergeur au sens juridique du terme. Dans le cadre de ses prestations, ITALIC contractualise avec des hébergeurs tiers (tels que Scaleway, OVH, AWS, etc.) pour le compte de ses Clients.

ITALIC met en œuvre des mesures de protection active et passive (surveillance, durcissement, sauvegardes) adaptées à ses prestations. Toutefois, il appartient au **Client** de réaliser ou de faire réaliser des audits de sécurité de l'hébergement. ITALIC se tient à disposition des auditeurs mandatés par le Client et coopérera pleinement avec eux.

8.2. Résilience et continuité d'activité

ITALIC dispose d'un **Plan de Reprise d'Activité (PRA)** permettant de réinstaller les applications hébergées à partir de sauvegardes récentes. ITALIC réalise **au minimum deux sauvegardes par jour dans deux zones géographiques distinctes**, espacées de 12 heures.

ITALIC s'engage à une **disponibilité minimale de 99 %**, correspondant à des durées maximales de downtime indicatives de :

- ~14 minutes par jour,
- ~1h40 par semaine,
- ~7h par mois,
- ~3,5 jours par an.

En cas de **crise majeure** (cyberattaque massive, incident critique touchant un éditeur de logiciel tiers ou un hébergeur, catastrophe naturelle, etc.), l**a SLA (Service Level Agreement)** exprimée en pourcentage de disponibilité ne constitue **pas une Garantie de Temps d'Intervention (GTI)**.

ITALIC s'engage à mobiliser tous les moyens raisonnables pour rétablir le service dans les meilleurs délais, mais sans engagement de délai fixe en dehors des engagements contractuellement souscrits auprès des hébergeurs tiers.

ITALIC reste toutefois tributaire :

- des logiciels tiers utilisés (WordPress, PrestaShop, Drupal, Symfony, etc.),
- des hébergeurs tiers (Scaleway, OVH, AWS, etc.) lorsqu'elle assure l'hébergement.

9. Qualité du code

9.1. Bonnes pratiques

Dans le cadre de son **obligation de moyens**, ITALIC applique les bonnes pratiques de développement (veille technique, recommandations de l'ANSSI, OWASP, etc.).

Néanmoins, il appartient au **Client** de faire auditer les livrables (code source, configurations). En cas de non-conformité objectivée par un audit indépendant, ITALIC corrigera gracieusement le code dans le cadre de son **obligation de résultat**.

9.2. Éco-conception et accessibilité

ITALIC maîtrise les référentiels publiés par l'État français (RGAA pour l'accessibilité numérique, référentiels d'éco-conception). Par défaut, ITALIC applique une approche **best effort** sur ces sujets, sans garantie de conformité intégrale.

La conformité stricte à ces référentiels implique un coût supplémentaire, devant être intégré au périmètre contractuel du projet et supporté par le Client. Dans ce cadre :

- Le Client peut mandater ses propres audits,
- Ou demander à ITALIC de faire réaliser des audits tiers, moyennant supplément,
- Lorsque ITALIC s'est contractuellement engagé sur la conformité, les défauts identifiés seront corrigés dans le cadre de son **obligation de résultat**.

10. Assurance professionnelle

ITALIC est couvert par une assurance professionnelle **Hiscox – Police HSXIN320030700M** « Métiers de l'Informatique et du Digital », applicable dans le monde entier (hors USA et Canada).

Cette police couvre l'activité **développement web et applications mobiles**, avec une garantie de **200 000 € par sinistre**.

Étant donné qu'ITALIC n'est pas hébergeur, les garanties spécifiques au métier d'hébergeur relèvent exclusivement des **conditions contractuelles de l'hébergeur** choisi.

Pour ITALIC
Germain Guglielmetti
Gérant – Responsable du traitement

Délégué à la Protection des Données (DPO)
Signature électronique :