SYNTHÈSE CYBERSÉCURITÉ · BTS SIO SISR

CentreCall : protéger les données personnelles d'un centre d'appels (RGPD)

Recenser les traitements, évaluer les risques, choisir les mesures de sécurité et organiser la conformité d'un centre d'appels, du point de vue du prestataire informatique.

Auteur	Plot 1
Contexte	Étude de cas CentreCall — centre d'appels traitant des données de clients et de prospects
Rôle étudié	Prestataire SI (infrastructure et applications) — sous-traitant au sens du RGPD
Version	2.0 — novembre 2026
Références	RGPD (règlement UE 2016/679), loi Informatique et Libertés, recommandations CNIL

Sommaire

1. Objectif et rôles
2. Recenser les traitements
3. Bases légales et durées
4. Cartographier les risques
5. Mesures de sécurité
6. AIPD
7. Droits des personnes
8. Violation de données
9. Sensibilisation
10. Check-list

1. Objectif et rôles

CentreCall passe et reçoit des appels pour le compte de clients (études de marché, prospection, service client). Chaque appel produit des données personnelles : identité, coordonnées, réponses, enregistrements audio. L'objectif est de garantir que ces données sont collectées légalement, protégées et supprimées à temps.

Acteur	Rôle RGPD	Obligations principales
Client donneur d'ordre	Responsable de traitement (ou conjoint avec CentreCall)	Définit la finalité, choisit la base légale, informe les personnes
CentreCall	Responsable ou sous-traitant selon la mission	Registre, sécurité, respect des instructions, gestion des droits
Prestataire SI (nous)	Sous-traitant (art. 28)	Contrat écrit, sécurité (art. 32), confidentialité, alerte en cas de violation
DPO	Délégué à la protection des données (art. 37)	Conseille, contrôle la conformité, point de contact de la CNIL

À savoir

Une donnée personnelle est toute information qui permet d'identifier une personne, directement (nom) ou indirectement (numéro de téléphone, voix enregistrée, identifiant client).

2. Recenser les traitements

Première étape : tenir le **registre des activités de traitement** (art. 30). Une fiche par traitement.

Traitement	Données	Finalité	Destinataires
Fichier de prospects	Nom, téléphone, adresse, âge	Prospection commerciale	Téléconseillers, client
Études de marché	Réponses aux questionnaires	Statistiques pour le client	Analystes, client (données agrégées)
Enregistrement des appels	Voix, date, durée, numéro	Formation, qualité de service, preuve	Superviseurs
Gestion du personnel	Comptes, plannings, statistiques d'appels	Organisation du travail	Managers, RH

Données sensibles (art. 9)

Santé, opinions politiques ou religieuses, orientation sexuelle… Leur traitement est interdit par principe. Un questionnaire ne doit pas en collecter sans consentement explicite. Ne pas confondre donnée personnelle (toute donnée identifiante) et donnée sensible (catégorie particulière).

3. Bases légales et durées de conservation

Chaque traitement doit reposer sur une des bases légales de l'article 6.

Traitement	Base légale	Durée de conservation indicative
Prospection téléphonique	Intérêt légitime ou consentement, avec droit d'opposition (liste Bloctel)	3 ans après le dernier contact
Études de marché	Consentement ou intérêt légitime	Durée de l'étude, puis anonymisation
Enregistrement des appels	Intérêt légitime (formation, qualité)	6 mois maximum (CNIL)
Journaux techniques	Obligation de sécurité	6 mois à 1 an

Information des personnes

Dès le début de l'appel : identité de l'appelant, finalité, enregistrement éventuel et possibilité de s'y opposer, droits et contact du DPO.

4. Cartographier les risques

Pour chaque menace, on évalue l'impact sur les trois critères **DIC** : disponibilité, intégrité, confidentialité.

Menace	Critère touché	Gravité	Mesure principale
Usurpation d'un compte de téléconseiller	Confidentialité	Élevée	MFA, comptes nominatifs, verrouillage de session
Export massif du fichier clients	Confidentialité	Élevée	Droits d'export limités, journalisation, alertes
Suppression volontaire de données	Intégrité, disponibilité	Moyenne	Sauvegardes, moindre privilège, traçabilité
Rançongiciel sur les serveurs	Disponibilité	Élevée	Sauvegardes hors ligne, correctifs, segmentation réseau
Écoute non autorisée des enregistrements	Confidentialité	Moyenne	Accès réservé aux superviseurs, chiffrement

5. Mesures de sécurité (art. 32)

1 Contrôle des accès

- Comptes nominatifs, aucun compte partagé
- MFA pour les accès à distance et aux outils d'administration
- Habilitations selon le principe du moindre privilège, revues chaque trimestre
- Désactivation des comptes dès le départ d'un salarié

2 Protection des données

- Chiffrement des disques, des sauvegardes et des flux (TLS)
- Minimisation : ne collecter que les champs utiles
- Pseudonymisation des données utilisées pour les statistiques
- Purge automatique à la fin de la durée de conservation

3 Traçabilité et continuité

- Journalisation des connexions, consultations et exports
- Sauvegardes selon la règle 3-2-1, avec une copie hors ligne testée régulièrement
- Mises à jour de sécurité appliquées rapidement
- Segmentation du réseau : postes de téléconseillers séparés des serveurs

6. Analyse d'impact (AIPD / PIA)

L'AIPD (art. 35) est obligatoire lorsqu'un traitement présente un **risque élevé** pour les droits et libertés des personnes, pas pour tous les traitements. En pratique, elle est requise dès que le traitement remplit au moins deux des critères du CEPD, par exemple : données à grande échelle, personnes vulnérables, croisement de fichiers, surveillance systématique.

- Décrire le traitement : contexte, finalités, données, durées, acteurs
- Vérifier les principes : base légale, minimisation, information, droits
- Évaluer les risques : accès illégitime, modification non désirée, disparition
- Valider le plan d'action, avec l'avis du DPO

> **Outil**
> La CNIL fournit gratuitement le logiciel PIA pour mener et documenter l'analyse.

7. Droits des personnes

Droit	Exemple chez CentreCall
Accès (art. 15)	Un prospect demande quelles données sont détenues sur lui
Rectification (art. 16)	Corriger un numéro ou une adresse erronés
Effacement (art. 17)	Supprimer la fiche d'une personne qui le demande
Opposition (art. 21)	« Ne plus m'appeler » : inscription immédiate sur la liste d'exclusion

> **Délai de réponse**
> 1 mois à compter de la demande, prolongeable de 2 mois si la demande est complexe, en prévenant la personne.

8. Violation de données

1 Détecter et contenir

Isoler les systèmes touchés, révoquer les accès compromis, conserver les journaux. Le prestataire SI alerte immédiatement le responsable de traitement.

2 Notifier

Le responsable de traitement notifie la CNIL **dans les 72 heures** (art. 33) si la violation présente un risque. Si le risque est élevé, il informe aussi les personnes concernées (art. 34).

3 Documenter

Inscrire chaque violation dans le registre interne, même sans notification : faits, effets, mesures prises.

9. Sensibilisation des équipes

- Ne jamais partager son identifiant, verrouiller son poste dès qu'on s'absente
- Ne noter dans les commentaires que des informations utiles et objectives
- Annoncer clairement l'enregistrement et la finalité de l'appel
- Reconnaître l'hameçonnage et les fausses demandes d'export
- Signaler tout incident sans délai au référent sécurité ou au DPO

10. Check-list de conformité

Point de contrôle	Article
Registre des traitements à jour	Art. 30
Base légale définie pour chaque traitement	Art. 6
Information des personnes au début de l'appel	Art. 13
Durées de conservation et purge automatique	Art. 5
Contrat de sous-traitance signé avec le prestataire SI	Art. 28
Mesures de sécurité adaptées et testées	Art. 32
AIPD réalisée si risque élevé	Art. 35
Procédure de gestion des violations	Art. 33-34

Sources : règlement (UE) 2016/679 (RGPD), cnil.fr (guides centres d'appels, sécurité des données, AIPD). Synthèse rédigée à partir d'une étude de cas réalisée en cours.