PROGRAMME D'EXCELLENCE EN CYBERSECURITE — APSI-NE x ACRC

COURS SPECIALISE — MODULE GRC / M04

PROTECTION DES DONNEES PERSONNELLES

Cadre juridique africain • Droits des personnes • Obligations des organisations

RGPD comme référence mondiale • Lois nationales africaines • DPO • EIPD

Cours	Protection des Données Personnelles — Fondements, cadre africain et mise en pratique
Programme	Programme d'Excellence en Cybersécurité — Cohorte 2026 — APSI-NE x ACRC
Module	M04 — Gouvernance, Risques et Conformité (GRC) — Spécialisation Protection des Données
Référentiels	RGPD (UE) 2016/679 • Lois nationales africaines • Convention de Malabo (UA) • ISO 27701
Public cible	Professionnels GRC, DPO en devenir, juristes numériques, responsables conformité
Certifications	AFP-Gouv Foundation (ACRC) • Prérequis pour spécialisation DPO africain
Structure	5 parties • 12 chapitres • Quiz 15 QCM • Cas pratique • Lexique complet

COMPETENCES VISEES

- Qualifier une donnée personnelle et distinguer les catégories de données
- Identifier les 6 bases légales du traitement et choisir la plus adaptée
- Maitriser les 10 droits des personnes concernées et gérer les demandes
- Mettre en place un registre des traitements conforme
- Conduire une Etude d'Impact relative a la Protection des Données (EIPD/DPIA)
- Gérer une violation de données : notification, communication, remédiation
- Nommer et encadrer un DPO (Délégué a la Protection des Données)
- Naviguer dans le paysage réglementaire africain de la protection des données

Niamey / Dakar — Cohorte 2026 — Document pedagogique confidentiel — Usage formation exclusif

INTRODUCTION — POURQUOI LA PROTECTION DES DONNEES ?

Chaque jour, des millions de citoyens africains confient leurs données personnelles a des organisations : banques, operateurs mobile, fintechs, administrations, hôpitaux, réseaux sociaux. Ces données noms, numéros de téléphone, transactions financières, localisations, données de sante ont une valeur immense. Et leur mauvaise gestion a des conséquences réelles sur des vies réelles.

La protection des données personnelles n'est pas une contrainte bureaucratique. C'est un droit fondamental de la personne humaine le droit de contrôler les informations qui la concernent. C'est aussi, pour les organisations, une obligation légale croissante et un enjeu de confiance décisive.

> ***"Les données personnelles sont le pétrole du XXIe siècle. Mais comme le pétrole, elles peuvent être une richesse ou une source de catastrophes si elles sont mal gérées."*** —
> *Aboubacar YACOUBA MAI BIRNI, President APSI-NE*

◆ Le paradoxe africain

L'Afrique est paradoxalement a la fois en retard et en avance sur ce sujet. En retard parce que de nombreux pays ne disposent pas encore d'une loi complète de protection des données. En avance parce que la transformation numérique africaine mobile money, e-gouvernement, fintechs crée des écosystèmes de données massifs qui nécessitent une protection urgente.

FOCUS AFRIQUE — L'Afrique face a la protection des donnees

54 pays africains environ 35 disposent d'une loi ou d'un projet de loi sur la protection des données personnelles (2025)

La Convention de Malabo (2014) de l'Union Africaine est le premier instrument panafricain ratifiée par trop peu de pays pour entrer en vigueur

Le RGPD européen influence directement les lois africaines : Senegal, Niger, Togo, Cote d'Ivoire, Maroc, Tunisie s'en sont fortement inspires

Le secteur financier africain traite des données de 400+ millions de clients une exposition massive sous-règlementée

Les violations de données dans le secteur bancaire africain sont en hausse de 35% par an selon les estimations disponibles

PARTIE I —

FONDEMENTS DE LA PROTECTION DES DONNEES

Concepts, définitions et principes universels

Chapitre 1 — Qu'est-ce qu'une donnée personnelle ?

DEFINITION — Donnee a caractere personnel

Toute information se rapportant a une personne physique identifiée ou identifiable. Une personne est identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence a un identifiant tel que son nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou a un ou plusieurs éléments spécifiques propres a son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

◆ Les types de données personnelles

Type	Définition	Exemples africains
Données d'identification directe	Permettent d'identifier directement la personne sans autre information	*Nom, prénom, numéro CNI/passeport, numéro de compte bancaire, adresse email*
Données d'identification indirecte	Permettent d'identifier la personne par croisement avec d'autres données	*Numéro de téléphone, adresse IP, cookie, numéro de plaque d'immatriculation, code postal*
Données sensibles (categorie spéciale)	Protection renforcée traitement principe interdit sauf exceptions	*Données biométriques (empreinte digitale pour ouverture de compte), sante, origine ethnique, opinions politiques, religion*
Données pseudonymies	Séparées de l'identité directe mais ré-identifiables avec une clé	*Numéro client anonymise mais lie a une base séparée permettant la re-identification*
Données anonymisées	Séparées DEFINITIVEMENT de l'identité ne sont PLUS des données personnelles	*Statistiques agrégées sur les transactions sans possibilité de relier a un individu*
Données des mineurs	Protection renforcée consentement parental requis sous un certain Age	*Données scolaires, profils sur réseaux sociaux, comptes d'épargne pour mineurs*

◆ Donnees sensibles — traitement exceptionnel

Certaines catégories de données font l'objet d'une protection renforcée car leur traitement peut engendrer des discriminations ou des préjudices graves. En principe, leur traitement est INTERDIT sauf exceptions strictes.

Origines raciales ou ethniques	Interdit sauf consentement explicite ou raison d'intérêt public majeur
Opinions politiques	Interdit sauf consentement explicite ou cadre syndical/associatif
Croyances religieuses ou philosophiques	Interdit sauf consentement explicite ou nécessite absolue
Appartenance syndicale	Interdit sauf nécessite pour la gestion des relations syndicales
Données de sante	Interdit sauf soins médicaux, intérêt public en sante, recherche
Données génétiques	Interdit sauf recherche scientifique avec garanties appropriées
Données biométriques (a des fins d'identification unique)	TRES COURANT EN AFRIQUE Empreintes pour mobile money, iris, reconnaissance faciale nécessite base légale spécifique
Données concernant la vie sexuelle	Interdit sauf consentement explicite
Données relatives aux infractions pénales	Reserve aux autorités judiciaires et administratives compétentes

FOCUS AFRIQUE — La biometrie en Afrique — une zone de risque majeure

La reconnaissance d'empreintes digitales est utilisée massivement pour l'enregistrement SIM, l'ouverture de comptes bancaires (KYC), les systèmes de vote électronique et les programmes d'aide sociale dans de nombreux pays africains.

Ces données biométriques sont des données sensibles selon toutes les législations. Leur collecte massive sans base légale adéquate ni mesures de sécurité appropriées crée un risque systémique pour des millions de citoyens africains.

Le vol ou la fuite de données biométriques est irréversible on ne peut pas changer ses empreintes digitales comme on change un mot de passe.

◆ Ce qui n'est PAS une donnée personnelle

- Les données anonymisées IRREVERSIBLEMENT ou l'identification est techniquement impossible (pas seulement difficile)
- Les données relatives à des personnes morales (entreprises, associations) sauf si elles permettent d'identifier les personnes physiques derrière
- Les données relatives à des personnes décédées sauf si les lois nationales le prévoient
- Les données purement internes à un usage strictement personnel et domestique

ATTENTION — Pseudonymisation ≠ Anonymisation

La pseudonymisation (remplacer le nom par un code) ne supprime pas le caractère personnel de la donnée si une clé de re-identification existe, même séparément. Les données pseudonymisees restent des données personnelles. Seule l'anonymisation irréversible (statistiques agrégées, differential privacy) sort les données du champ de la régulation.

Chapitre 2 — Les 10 principes fondamentaux

Les principes fondamentaux de la protection des données sont universels ils se retrouvent dans le RGPD européen, les lois africaines, la Convention de Malabo et les lignes directrices de l'OCDE. Tout traitement de données personnelles doit respecter l'ensemble de ces principes simultanément.

PRINCIPE 1 — LICÉITÉ, LOYAUTE ET TRANSPARENCE

Les données doivent être traitées de manière licite (sur la base d'une des 6 bases légales), loyale (sans tromper la personne) et transparente (la personne sait comment ses données sont utilisées). Ce principe impose des obligations d'information claires.

- **Licite :** il existe une base légale valable pour le traitement (voir Chapitre 3) ;
- **Loyal :** les données ne sont pas collectées a l'insu de la personne ou de manière trompeuse ;
- **Transparent :** la personne reçoit une information claire, accessible et compréhensible sur le traitement.

PRINCIPE 2 — LIMITATION DES FINALITES

Les données ne peuvent être collectées que pour des finalités déterminées, explicites et légitimes. Elles ne peuvent ensuite être traitées de manière incompatible avec ces finalités initiales.

EXEMPLE — Exemple : violation de la limitation des finalites

Une banque collecte les données de ses clients pour gérer leurs comptes et exécuter leurs transactions (finalité 1). Si cette banque utilise ensuite ces mêmes données pour vendre des profils comportementaux a des annonceurs publicitaires (finalité 2), elle viole le principe de limitation des finalités. La finalité 2 est incompatible avec la finalité 1.

En revanche, utiliser ces mêmes données pour détecter des fraudes sur les comptes de ces mêmes clients (finalité 3) peut être considère comme compatible avec la finalité initiale car c'est dans l'intérêt du client.

PRINCIPE 3 — MINIMISATION DES DONNEES

Les données collectées doivent être adéquates, pertinentes et limitées a ce qui est nécessaire au regard des finalités. On ne collecte pas de données 'au cas ou' ou 'parce que c'est possible'.

- **Adequates :** les donnees couvrent bien la finalité (suffisantes pour l'objectif) ;
- **Pertinentes :** chaque donnee collectee est directement liee a la finalite ;
- **Limitees au necessaire :** pas de collecte excessive ou inutile.

PRINCIPE 4 — EXACTITUDE

Les donnees personnelles doivent etre exactes et si necessaire tenues à jour. Des mesures raisonnables doivent etre prises pour effacer ou rectifier les donnees inexactes. Ce principe alimente directement le droit de rectification des personnes concernees.

PRINCIPE 5 — LIMITATION DE LA CONSERVATION

Les donnees ne peuvent etre conservees que le temps necessaire a la realisation des finalites. Au-dela, elles doivent etre supprimees ou anonymisees de maniere irreversible.

Donnees de KYC bancaires (identite client)	Duree de la relation client + 10 ans (obligations LCBFT)
Donnees de transactions bancaires	10 ans (obligations comptables et reglementaires BCEAO)
Donnees de candidatures non retenues	6 mois a 2 ans selon les pays (droit du travail)
Cookies de mesure d'audience	13 mois maximum selon les recommandations CNIL
Logs de connexion/securite	Entre 1 et 5 ans selon les reglementations sectorielles
Donnees de sante	Durée de prise en charge + 20 ans (selon legislations nationales)

PRINCIPE 6 — INTEGRITE ET CONFIDENTIALITE

Les donnees doivent etre traitees avec un niveau de securite approprie protection contre le traitement non autorise, la perte accidentelle, la destruction ou l'endommagement. Ce principe etablit le lien direct entre protection des donnees et cybersecurite.

En pratique, ce principe implique la mise en place des controles ISO 27001 Annexe A pertinents : chiffrement, controle d'acces, pseudonymisation, journalisation, etc.

PRINCIPE 7 — RESPONSABILITE (ACCOUNTABILITY)

Le responsable du traitement est responsable du respect de tous les principes précédents et doit etre en mesure de le DEMONTRER. Ce principe transforme la protection des donnees d'une obligation de comportement en une obligation de documentation et de preuve.

- Tenir un registre des traitements a jour ;
- Realiser des EIPD pour les traitements a risque ;
- Mettre en oeuvre les mesures techniques et organisationnelles appropriees ;
- Former et sensibiliser le personnel ;
- Documenter toutes les decisions relatives à la protection des donnees.

A RETENIR

- **7 principes fondamentaux :** Licéité/Loyaute/Transparence, Finalites, Minimisation, Exactitude, Conservation limitee, Integrite/Confidentialite, Responsabilite ;
- Ces principes sont cumulatifs un traitement doit les respecter TOUS simultanément ;
- **Le principe de minimisation :** collecter uniquement ce qui est NECESSAIRE pas ce qui est POSSIBLE ;
- La limitation de conservation oblige à definir des durees de retention et a les respecter ;
- L'accountability exige de documenter la conformite ne pas seulement se conformer mais PROUVER qu'on se conforme.

Chapitre 3 — Les bases legales du traitement

Un traitement de donnees personnelles n'est licite que s'il repose sur l'une des bases legales reconnues par la loi applicable. Choisir la bonne base legale est une decision juridique fondamentale elle determine les droits des personnes concernees et les obligations du responsable du traitement.

ATTENTION — Choisir la bonne base legale une decision irrevocable

On ne peut pas changer de base legale en cours de traitement. Si on a choisi le consentement, on ne peut pas invoquer ulterieurement l'interet legitime si les personnes retirent leur consentement. Il faut choisir la base legale correcte DES LE DEBUT du traitement, lors de la conception.

◆ Les 6 bases legales

Base legale	Definition	Conditions	Exemple africain
1 — CONSENTEMENT	La personne a donne son accord libre, specifique, eclaire et univoque	Doit etre granulaire, revocable a tout moment, prouve par l'organisation	Client qui coche une case pour recevoir des offres promotionnelles par SMS
2 — CONTRAT	Le traitement est necessaire a l'execution d'un contrat avec la personne concernee	La personne doit etre partie au contrat pas un tiers	Traitement des donnees bancaires pour executer les virements contractuellement prevus
3 — OBLIGATION LEGALE	Le traitement est impose par une loi ou reglementation applicable	La loi doit etre precise et previsible	Collecte des donnees KYC imposee par les lois anti-blanchiment (LCBFT/BCEAO)
4 — INTERET VITAL	Le traitement est necessaire pour proteger les interets vitaux de la personne ou d'un tiers	Uniquement en cas d'urgence ou impossibilite d'obtenir le consentement	Transmission de donnees medicales en cas d'urgence hospitaliere
5 — MISSION D'INTERET PUBLIC	Le traitement est necessaire a l'execution d'une mission d'interet public	Reserve principalement aux autorites publiques	Recensement national, statistiques publiques, registre de l'etat civil
6 — INTERET LEGITIME	Le traitement est necessaire aux interets legitimes de l'organisation sauf si primé par les droits des personnes	Doit passer le test de balance des interets ne s'applique pas aux autorites publiques	Detection des fraudes sur les comptes clients, securite informatique, analyses internes

◆ Focus : le consentement — conditions de validite

Le consentement est souvent invoque a tort comme base legale par defaut. En realite, un consentement valide est soumis a des conditions strictes :

LIBRE	Pas de consequence negative si refus. Le service ne peut pas etre conditionne au consentement a des traitements non necessaires. Le desequilibre de pouvoir **(employeur/employe)** invalide le consentement.
SPECIFIQUE	Un consentement par finalite distincte. Pas de consentement global pour tout faire. Chaque traitement distinct necessite un consentement separe.
ECLAIRE	La personne doit comprendre ce a quoi elle consent : qui traite, pour quoi, combien de temps, qui a acces. L'information doit etre en langage clair.
UNIVOQUE	Action positive et deliberee (cliquer sur 'J'accepte'). Pas de cases pre-cochees, pas de consentement par silence ou inaction.
REVOCABLE	La personne peut retirer son consentement a tout moment aussi facilement qu'elle l'a donne. Le retrait ne remet pas en cause la licéite des traitements anterieurs.
DOCUMENTABLE	L'organisation doit pouvoir PROUVER que le consentement a ete donne : date, heure, version de la politique, cases cochees. Obligation de conservation de la preuve.

FOCUS AFRIQUE — Le consentement en contexte africain — defis pratiques

Dans de nombreux pays africains, les formulaires de consentement sont en francais juridique ou en anglais, incomprehensibles pour des personnes peu alphabetisees. Un consentement « **eclaire** » suppose une information accessible dans les langues locales et a un niveau de comprehension adapte.

La relation de dependance economique (client vulnerable / banque unique de la zone, beneficiaire d'aide sociale / Etat) cree un desequilibre de pouvoir qui compromet la liberte du consentement. Le RGPD reconnait explicitement ce probleme pour la relation employe/employeur.

PARTIE II —

LE CADRE REGLEMENTAIRE AFRICAIN

Lois nationales, autorites de controle et specificites sectorielles

Chapitre 4 — Panorama des lois africaines

L'Afrique n'est pas un desert juridique en matiere de protection des donnees. Au contraire, le continent connait depuis 2015 une acceleration remarquable des legislations. Ces lois s'inspirent largement du RGPD europeen (2016/679) et de la Convention 108 du Conseil de l'Europe, tout en tenant compte des specificites africaines.

◆ Les lois par pays — UEMOA et CEMAC

Pays	Loi / Texte principal	Autorite de controle	Specificites notables
SENEGAL	Loi n°2008-12 du 25 janvier 2008 sur la Protection des Donnees a Caractere Personnel	**CDP** — Commission des Donnees Personnelles	Premiere loi complete en Afrique francophone. Obligation de declaration. DPO pour secteur public.
NIGER	Loi n°2020-037 du 17 juillet 2020 portant protection des DCP + Decret d'application	**ANPDP** — Autorite Nationale de Protection des Donnees Personnelles	Inspiree RGPD. Notification 72h. DPO obligatoire. Sanctions penales renforcees.
COTE D'IVOIRE	Loi n°2013-450 du 19 juin 2013 relative a la protection des donnees a caractere personnel	**ARTCI** — Autorite de Regulation des Telecommunications	Autorisation prealable pour certains traitements. 5 ans de prison possible.
BURKINA FASO	Loi n°010-2004 sur la protection des donnees a caractere personnel (en revision)	**CIL** — Commission de l'Informatique et des Libertes	Ancienne loi, reforme en cours pour alignement RGPD. Declaration obligatoire.
TOGO	Loi n°2019-014 du 29 octobre 2019 relative a la protection des donnees a caractere personnel	**ARDP** — Autorite de Regulation et de Protection des Donnees	Tres proche du RGPD. DPO, EIPD, notification 72h, portabilite.
BENIN	Loi n°2009-09 du 22 mai 2009 portant protection des DCP	**APDP** — Autorite de Protection des Donnees Personnelles	Autorisation préalable pour traitements sensibles. Sanctions pénales.
MALI	En cours d'élaboration (2024-2025)	Pas d'autorite independante constituee	Vide juridique partiel — application des textes CEDEAO

Pays	Loi / Texte principal	Autorite de controle	Specificites notables
CAMEROUN	Loi n°2010-012 du 21 decembre 2010 relative a la cybersecurite (volet donnees)	**ANTIC** — Agence Nationale des TIC	Loi cybersecurite avec volet donnees. Regime CEMAC distinct.
TCHAD	Loi n°007/PR/2015 relative a la cybersecurite (volet donnees)	**ANIC** — Agence Nationale de l'Informatique	Cadre partiel en cours de renforcement
GABON	Loi n°001/2011 relative a la protection des donnees a caractere personnel	**CNPD** — Commission Nationale de Protection des Donnees	Loi complete, autorite independante, inspiration senegalaise

◆ Les instruments regionaux et internationaux

Convention de Malabo (Union Africaine) — 2014	Premier instrument panafricain sur la cybersecurite et la protection des donnees. Adoptee par 14 pays mais necessite 15 ratifications pour entrer en vigueur. Principe d'adequation pour les transferts.
Acte Additionnel CEDEAO A/SA.1/01/10	Acte additionnel sur la protection des donnees personnelles entre Etats membres de la CEDEAO. Harmonisation des niveaux de protection en Afrique de l'Ouest.
Convention 108+ du Conseil de l'Europe	Ouverte aux pays non-membres du Conseil de l'Europe. Plusieurs pays africains ont adhere (Maroc, Tunisie, Cap-Vert, Senegal en cours). Modernisee en 2018 (Convention 108+).
RGPD (UE) 2016/679	Applicable aux organisations africaines qui traitent des donnees de residents europeens ou qui ciblent le marche europeen. Extraterritorialite importante pour les banques correspondantes et les fintechs exportatrices.
Lignes directrices OCDE sur la vie privee	Reference internationale (non contraignante) adoptee en 1980, revisee en 2013. Base des legislations nationales mondiales.

◆ Le RGPD comme reference mondiale — extraterritorialite

Meme sans loi nationale complete, de nombreuses organisations africaines sont soumises au RGPD europeen par son effet extraterritorial (article 3 RGPD). Le RGPD s'applique a toute organisation qui :

- Traite des donnees de personnes physiques qui se trouvent dans l'UE (clients, partenaires, prestataires) ;
- Propose des biens ou services a des personnes dans l'UE (meme gratuitement) ;
- Surveille le comportement de personnes dans l'UE (cookies, tracking).

FOCUS AFRIQUE — Quelles organisations africaines sont concernees par le RGPD ?

Banques correspondantes : toute banque africaine ayant des relations avec des banques européennes traite des données de clients européens dans les virements SWIFT potentiellement concernée.

Fintechs exportatrices : une fintech sénégalaise proposant une application a la diaspora africaine en Europe est soumise au RGPD pour ces utilisateurs.

Prestataires de services IT : une ESN ivoirienne développant des logiciels pour des clients européens traite des données sous-traitance soumise au RGPD.

Hotels, tourisme : tout établissement accueillant des clients européens et gérant leurs réservations en ligne tombe potentiellement sous le RGPD.

Chapitre 5 — Les autorites de controle et les sanctions

Les autorites de controle (ou autorites de protection des donnees) sont des organes independants charges de veiller a l'application de la loi de protection des donnees dans leur pays. Elles disposent de pouvoirs importants.

◆ Pouvoirs des autorites de controle

Type de pouvoir	Description	Exemples d'exercice
Pouvoir d'enquete	Accès aux locaux, aux systèmes, aux documents. Audits, inspections sur place. Demandes d'information sous astreinte.	*Inspection surprise d'une banque suite a un signalement d'un employé*
Pouvoir correcteur	Avertissements, mises en demeure, injonctions de cesser un traitement, limitation ou interdiction d'un traitement, mise en conformité forcée.	*Injonction d'effacement de données illégalement collectées*
Pouvoir de sanction	Amendes administratives pouvant atteindre plusieurs millions de FCFA selon les pays. Sanctions pénales possibles.	*Amende pour absence de registre des traitements + violation non notifiée*
Pouvoir d'autorisation	Autorisation préalable pour certains traitements sensibles (biométrie, données de sante, surveillance des employés).	*Autorisation pour le déploiement d'un système de reconnaissance faciale*
Pouvoir consultatif	Avis sur les projets de loi et règlements ayant un impact sur la protection des données. Recommandations et lignes directrices.	*Avis sur le projet de loi sur l'identité numérique nationale*

◆ Sanctions — niveaux et exemples

Cadre juridique	Niveau de sanction maximum	Exemples de sanctions europeennes (reference)
RGPD (UE)	20 millions EUR OU 4% du chiffre d'affaires mondial le plus eleve des deux	*Meta : 1,2 Mrd EUR (Irlande, 2023) transferts illegaux vers les USA*
Togo — Loi 2019-014	5 millions FCFA (personnes morales) + emprisonnement possible	*Sanctions encore rares autorité ARDP en montée en puissance*
Niger — Loi 2020-037	De 500 000 a 50 millions FCFA selon la gravite + sanctions penales	*ANPDP opérationnelle depuis 2022 premières inspections en 2023-2024*
Cote d'Ivoire — Loi 2013-450	Jusqu'a 50 millions FCFA + 5 ans d'emprisonnement	*Sanctions principalement pénales instruction judiciaire possible*
Senegal — Loi 2008-12	De 500 000 a 25 millions FCFA + emprisonnement	*CDP active plusieurs décisions de mise en conformité rendues*

A RETENIR

- 35+ pays africains disposent d'une loi ou d'un projet de loi sur la protection des données (2025) ;
- La Convention de Malabo (UA) n'est pas encore en vigueur ratification insuffisante ;
- Le RGPD européen s'applique aux organisations africaines traitant des données de résidents UE effet extraterritorial ;
- Les autorités de contrôle africaines montent en puissance : inspections, sanctions, avis ne pas les ignorer ;
- En l'absence de loi nationale, les organisations africaines devraient appliquer le RGPD comme standard minimum

PARTIE III —

OBLIGATIONS DES ORGANISATIONS

Registre des traitements, DPO, EIPD et violations de donnees

Chapitre 6 — Le registre des traitements

DEFINITION — Registre des traitements

Document interne obligatoire listant l'ensemble des activités de traitement de données personnelles réalisées par une organisation. Il matérialise le principe d'accountability et constitue la carte d'identité de la conformité de l'organisation.

Le registre des traitements est LA base de la conformité en protection des données. Sans lui, impossible de savoir quelles données on traite, pour quoi, comment et ou. Il est obligatoire sous le RGPD et dans la plupart des lois africaines modernes (Togo, Niger, etc.).

◆ Contenu du registre des traitements

Pour chaque activité de traitement, le registre doit documenter :

Nom et description du traitement	Identifiant unique, intitule clair et description de l'activite (ex : ***« Gestion des comptes clients BSF »)***
Finalite(s)	Pourquoi ces donnees sont traitees doit etre specifique et legitime (ex : ***« Execution des contrats bancaires, lutte anti-fraude »)***
Base legale	Quelle base legale justifie le traitement (ex : ***« Contrat + Obligation legale LCBFT »***)
Responsable du traitement	Organisation responsable. Si plusieurs organisations : qui est responsable conjoint ou sous-traitant
Categories de personnes concernees	Qui est vise : clients, employes, prospects, mineurs...
Categories de donnees traitees	Quelles donnees : identite, donnees bancaires, biometrie, donnees de sante...
Destinataires	Qui a acces aux donnees : internes (departements), externes (prestataires, partenaires, regulateurs)
Transferts hors territoire	Vers quels pays les donnees sont transferees et sur quelle base legale
Durees de conservation	Combien de temps les donnees sont conservees pour chaque categorie

Mesures de securite	Description generale des mesures de securite techniques et organisationnelles (chiffrement, controle acces, pseudonymisation)

◆ Registre des traitements — exemple pour une banque africaine

ID / Traitement	Finalite / Base legale	Donnees et destinataires	Conservation / Securite
T-001 — KYC et ouverture de compte	Identification client, lutte anti-blanchiment / Obligation legale (BCEAO/LCBFT)	Identite, biometrie, revenus. Destinataires : agences, BCEAO, CTAF	10 ans apres cloture. Chiffrement AES-256, acces role-based
T-002 — Gestion des transactions	Execution des virements et paiements / Contrat	IBAN, montants, beneficiaires, dates. Destinataires : correspondants bancaires, SWIFT	10 ans. Logs securises, acces limité equipe transactionnel
T-003 — Mobile Money SahelPay	Service de paiement mobile / Contrat + Consentement pour donnees marketing	Tel, localisation (transactions), historique. Dest. : partenaires paiement	5 ans apres derniere transaction. Pseudonymisation des logs
T-004 — Surveillance anti-fraude	Detection et prevention de fraude / Interet legitime	Transactions, comportements, score de risque. Dest. : equipe fraude, BCEAO	3 ans. Acces strictement limite a l'equipe fraude
T-005 — RH — Gestion du personnel	Gestion des contrats de travail / Contrat + Obligation legale (droit du travail)	Identite, salaire, conges, evaluations. Dest. : RH, DAF, administration fiscale	Duree du contrat + 5 ans. Acces DRH uniquement
T-006 — Cookies et analytics site web	Mesure d'audience / Consentement	Adresse IP, pages visitees, duree. Dest. : equipe marketing, Google Analytics	13 mois. Anonymisation des IP, bandeau cookies conforme

Chapitre 7 — Le Delegue a la Protection des Donnees (DPO)

DEFINITION — DPO — Delegue a la Protection des Donnees

Le DPO (Data Protection Officer ou Delegue a la Protection des Donnees) est un profil expert, nomme par une organisation pour superviser sa strategie de protection des donnees et assurer la conformite avec les lois applicables. Il est a la fois un conseiller technique, un juriste, un formateur et un interlocuteur privilegie des autorites de controle.

◆ Quand le DPO est-il obligatoire ?

Le RGPD rend le DPO obligatoire dans trois cas. Les lois africaines modernes (Togo, Niger notamment) reprennent ce principe :

Autorite ou organisme public	Toute autorite publique ou organisme public doit nommer un DPO (sauf juridictions dans leurs fonctions)
Traitement a grande echelle de donnees sensibles	Traitements de donnees de sante, biometriques, genetiques, relatives aux infractions a grande echelle
Traitement a grande echelle avec suivi regulier et systematique	Profilage de consommateurs, suivi de localisation, surveillance des employes, scoring bancaire

FOCUS AFRIQUE — Le DPO dans le secteur financier africain

TOUTES les banques de la zone UEMOA et CEMAC devraient avoir un DPO (ou un profil equivalent). Elles traitent a grande echelle des donnees sensibles (biometrie KYC), effectuent un suivi systematique (transactions, scoring de credit) et sont soumises a des obligations reglementaires fortes.

En pratique, la quasi-totalite des banques africaines n'ont pas de DPO nomme en 2024. C'est une lacune majeure et une opportunite de carriere exceptionnelle pour les professionnels formes.

Le DPO peut etre interne (employe dedié) ou externe (consultant/cabinet). Pour les PME et les banques de taille moyenne, le DPO externe mutualisé est une solution pragmatique.

◆ Les missions du DPO

Mission	Description	Livrables types
Information et conseil	Informer et conseiller l'organisation et ses employes sur leurs obligations en matiere de protection des donnees	*Notes juridiques, avis sur les projets, formations*
Controle de la conformite	Verifier que les traitements respectent les obligations legales. Piloter le registre des traitements. Auditer les processus.	*Rapports d'audit interne, tableau de bord conformite*

Mission	Description	Livrables types
Conseil sur l'EIPD	Conseiller sur la realisation des etudes d'impact. Verifier leur qualite. Decider si une consultation de l'autorite est necessaire.	*Avis DPO sur les EIPD realisees*
Cooperation avec l'autorite	Etre le point de contact avec l'autorite de controle. Gerer les demandes d'inspection. Notifier les violations.	*Correspondance avec la CDP/ANPDP/ARDP, notifications de violations*
Point de contact des personnes	Gerer les demandes d'exercice de droits (acces, effacement, rectification...). Assurer les reponses dans les delais legaux.	*Suivi des demandes, reponses aux personnes concernees*
Sensibilisation et formation	Mettre en place le programme de sensibilisation des employes. Former les nouveaux arrivants.	*Modules de formation, attestations, registre de formation*

◆ Le profil du DPO

Le DPO doit avoir des connaissances etendues dans plusieurs domaines — c'est un profil hybride rare et tres demande :

- **Juridique :** droit de la protection des donnees national et international, droit des obligations, droit du numerique ;
- **Technique :** comprehension des systemes d'information, architectures IT, mesures de securite, chiffrement, controles d'acces ;
- **Organisationnel :** gestion de projet, communication, animation d'equipes transversales, reporting a la direction ;
- **Sectoriel :** connaissance approfondie du secteur de l'organisation (banque, sante, telecom...) et de ses specificites reglementaires.

BON A SAVOIR — L'independance du DPO — une condition essentielle

Le DPO ne peut pas recevoir d'instructions dans l'exercice de ses missions. Il ne peut pas etre penalise ou revoque pour avoir exerce ses fonctions. Il doit avoir acces aux ressources, a la formation et a la direction. Il ne peut pas etre en situation de conflit d'interets (il ne peut pas etre a la fois DPO et DSI, par exemple, dans une grande organisation).

Chapitre 8 — L'Etude d'Impact relative a la Protection des Donnees (EIPD)

DEFINITION — EIPD — Etude d'Impact sur la Protection des Donnees

L'EIPD **(ou DPIA en anglais Data Protection Impact Assessment)** est une analyse prospective et systematique menee AVANT le demarrage d'un traitement susceptible d'engendrer un risque eleve pour les droits et libertes des personnes. Elle evalue les risques et identifie les mesures pour les attenuer.

◆ Quand realiser une EIPD ?

L'EIPD est obligatoire lorsqu'un traitement est susceptible d'engendrer un risque ELEVE pour les droits et libertes des personnes. En pratique, elle est requise notamment quand :

Evaluation ou scoring systematique	Notation de credit, scoring comportemental, evaluation des performances des employes
Traitement automatise avec effets significatifs	Decisions automatisees affectant l'acces au credit, a l'emploi, aux assurances
Surveillance a grande echelle	Video-surveillance, monitoring des transactions, tracking de localisation continue
Donnees sensibles a grande echelle	KYC biometrique de millions de clients, donnees de sante, opinions politiques
Croisement ou combinaison de donnees	Fusion de bases de donnees permettant un profilage avance non prevu initialement
Donnees de personnes vulnerables	Traitements impliquant des mineurs, personnes agees, populations en situation de precarite
Technologies innovantes	Biometrie, IA de reconnaissance faciale, Internet des objets, CBDC (monnaie digitale de banque centrale)

◆ Les etapes de l'EIPD

Etape	Activites	Livrable
1 — Description du traitement	**Decrire le traitement :** finalites, personnes concernees, donnees collectees, processus, flux de donnees, sous-traitants, technologies utilisees	*Fiche descriptive du traitement, cartographie des flux de donnees*
2 — Evaluation de la necessite et proportionnalite	Verifier que le traitement est necessaire, proportionne et s'appuie sur une base legale valide. Verifier que les droits des personnes sont respectes	*Analyse de conformite aux principes et bases legales*

Etape	Activites	Livrable
3 — Identification et evaluation des risques	Identifier les risques pour les droits et libertes (acces non autorise, modification non desiree, disparition des donnees, discrimination...). Evaluer leur vraisemblance et leur gravite.	*Registre des risques EIPD avec cotation*
4 — Identification des mesures d'attenuation	Pour chaque risque identifie, definir des mesures techniques et organisationnelles pour le reduire. Evaluer le risque residuel apres mesures.	*Plan de traitement des risques EIPD*
5 — Validation et consultation	Si le risque residuel reste eleve apres mesures, consultation obligatoire de l'autorite de controle AVANT demarrage. Validation par le DPO.	*Avis DPO, eventuellement consultation de l'autorite*
6 — Revue periodique	L'EIPD n'est pas un document ponctuel elle doit etre revue si le traitement change significativement.	*EIPD mise a jour, journal des revisions*

EXEMPLE — EIPD pour un systeme de scoring de credit par IA de la banque africaine

Description : Une banque envisage de deployer un modele d'IA pour scorer automatiquement les demandes de credit des 750 000 clients, en utilisant les historiques de transactions, le comportement sur l'application mobile et des donnees tierces.

Risques identifies : Discrimination algorithmique (le modele peut discriminer involontairement selon le genre ou la zone geographique), opacite des decisions (clients rejetes sans explication), donnees d'entrainement biaisees, re-identification possible via les patterns de comportement.

Mesures d'attenuation : Audit de biais algorithmique regulier, obligation d'explicabilite (droit a l'explication des decisions automatisees), intervention humaine obligatoire sur les rejets, limitation des donnees d'entrainement aux donnees directement pertinentes.

Risque residuel : Eleve consultation de l'autorite de controle (ANPDP/CDP) requise avant deploiement.

Chapitre 9 — Gestion des violations de donnees

DEFINITION — Violation de donnees personnelles

Toute violation de la sécurité entrainant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorise à des données personnelles transmises, conservées ou traitées d'une autre manière. Une violation peut être une cyberattaque, une erreur humaine, une perte d'équipement ou tout autre incident.

◆ Types de violations

Type	Definition	Exemples africains
Violation de confidentialité	Accès ou divulgation non autorises de données a des personnes non habilitées	*Email avec données clients envoyé a un mauvais destinataire, fuite de la base KYC, accès d'un ancien employé*
Violation d'intégrité	Modification non autorisée ou non désirée de données	*Alteration de données de transaction par un employé malveillant, ransomware chiffrant les données*
Violation de disponibilité	Perte ou destruction accidentelle ou non autorisée de données	*Panne de disque dur sans sauvegarde, incendie de la salle serveurs, ransomware détruisant les données*

◆ Le processus de gestion d'une violation — les 72 heures

Le RGPD et les lois africaines modernes imposent une notification a l'autorité de contrôle dans les 72 heures apres avoir pris connaissance de la violation. Ce délai est très court il faut avoir préparé les procedures AVANT qu'une violation ne survienne.

Phase	Timing	Actions obligatoires
DETECTION	J + 0 h	*Identifier et isoler l'incident. Activer la procédure de violation de données. Alerter le DPO et le RSSI. Documenter la prise de connaissance (date et heure précises).*
QUALIFICATION	J + 0 a 24 h	*Determiner si la violation concerne des donnees personnelles. Evaluer le risque pour les personnes (negligeable, limite, important, maximal). Commencer la documentation de l'incident.*
NOTIFICATION AUTORITE	J + 72 h maximum	*Si risque non negligeable : notifier l'autorite de controle (CDP, ANPDP, ARDP selon le pays). La notification*

Phase	Timing	Actions obligatoires
		peut être incomplète et complétée ultérieurement. Ne pas attendre d'avoir toutes les informations.
COMMUNICATION AUX PERSONNES	Des que possible si risque ELEVE	*Si la violation est susceptible d'engendrer un risque ELEVE pour les droits et libertés, informer individuellement chaque personne concernée. Message clair, en langage non technique.*
REMEDIATION ET SUIVI	J + 0 a J + 30	*Mettre en œuvre les mesures correctives. Documenter toutes les actions. Analyser les causes racines. Adapter les procedures pour éviter la recurrence.*

ATTENTION — Les 72 heures — un delai qui ne pardonne pas

Ne pas notifier une violation dans le délai de 72 heures est en soi une infraction grave, indépendamment de la violation initiale. En 2023, British Airways a été sanctionnée 20 millions GBP pour ne pas avoir notifié dans les délais une violation affectant 500 000 passagers. En Afrique, les autorités commencent également à sanctionner les notifications tardives.

◆ Contenu de la notification a l'autorite de controle

Nature de la violation	Type (confidentialité/intégrité/disponibilité), catégories de données et de personnes concernées, nombre approximatif de personnes et d'enregistrements
Coordonnées du DPO	Nom, prénom, email, téléphone du DPO ou du point de contact pour les questions
Conséquences probables	Description des conséquences probables de la violation pour les personnes concernées
Mesures prises ou envisagées	Actions mises en œuvre ou planifiées pour remédier a la violation et en atténuer les conséquences

A RETENIR

- Le registre des traitements est la base de toute conformité sans lui, on ne sait pas ce qu'on protège ;
- Le DPO n'est pas le 'responsable si ça tourne mal il est le conseiller indépendant et le garant de la conformité ;
- L'EIPD est préventive elle doit être réalisée AVANT le démarrage d'un traitement a risque, pas apres ;
- 72 heures : c'est le délai maximum pour notifier l'autorité de contrôle après une violation préparer les procedures avant l'incident.

- La notification aux personnes concernées est requise si le risque pour leurs droits et libertés est ELEVE (pas seulement modère)

PARTIE IV —

DROITS DES PERSONNES CONCERNEES

Les 10 droits fondamentaux et leur gestion pratique

Chapitre 10 — Les 10 droits fondamentaux

Les lois de protection des données confèrent aux personnes concernées un ensemble de droits sur leurs données. Ces droits ne sont pas optionnels les organisations ont l'obligation de les respecter et de les faciliter. Elles doivent informer les personnes de ces droits et répondre à leurs demandes dans des délais précis (généralement 1 mois selon le RGPD, délais variables selon les lois africaines).

DROIT 1 — LE DROIT A L'INFORMATION

Toute personne dont les données sont collectées doit être informée, de manière claire et accessible, des éléments essentiels du traitement. Cette information doit être fournie AU MOMENT de la collecte.

Qui traite ses données	Identité et coordonnées du responsable du traitement (et du DPO si applicable)
Pour quoi	Finalités du traitement et base legale utilisée
Quelles données	Catégories de données collectées
Combien de temps	Durées de conservation ou critères pour les déterminer
A qui	Destinataires ou catégories de destinataires
Ses droits	Liste des droits applicables et comment les exercer
Les transferts	Si les données sont transférées hors du pays vers quels pays et sur quelle base

Cette information est généralement formalisée dans une POLITIQUE DE CONFIDENTIALITE (privacy notice) un document accessible, en langage clair, disponible sur le site web, dans les formulaires de collecte et dans les conditions contractuelles.

DROIT 2 — LE DROIT D'ACCES

Toute personne peut demander a l'organisation de lui communiquer une copie de toutes les données la concernant qui sont traitées, ainsi que des informations sur ce traitement (finalités, destinataires, durées de conservation...).

- La réponse doit être fournie dans un délai d'UN MOIS (RGPD) certaines lois africaines prévoient des délais différents ;
- La copie des données doit être fournie gratuitement dans un format compréhensible ;
- Si la demande est manifestement infondée ou excessive, l'organisation peut exiger un droit raisonnable ou refuser en justifiant.

DROIT 3 — LE DROIT DE RECTIFICATION

Toute personne peut demander la correction de données inexactes la concernant, ou le complément de données incomplètes. L'organisation doit effectuer la rectification sans delai indu et informer les éventuels destinataires auxquels les données ont été communiquées.

DROIT 4 — LE DROIT A L'EFFACEMENT (droit a l'oubli)

Toute personne peut demander la suppression de ses données dans certaines circonstances spécifiques :

- Les données ne sont plus nécessaires au regard des finalités initiales ;
- La personne retire son consentement et il n'existe pas d'autre base légale ;
- La personne s'oppose au traitement et il n'existe pas de motif légitime prépondérant ;
- Les données ont été traitées illicitement ;
- La suppression est imposée par une obligation légale.

BON A SAVOIR — Le droit a l'effacement n'est pas absolu

L'effacement peut être refuse si le traitement est nécessaire pour : l'exercice de la liberté d'expression, le respect d'une obligation légale (ex : conservation 10 ans des données bancaires), des raisons d'intérêt public, des fins de recherche, ou la constatation ou défense de droits en justice.

DROIT 5 — LE DROIT A LA LIMITATION DU TRAITEMENT

Toute personne peut demander la **« mise en pause »** du traitement de ses données sans effacement dans certains cas : contestation de l'exactitude, traitement illicite mais la personne refuse l'effacement, données plus nécessaires mais la personne en a besoin pour une action en justice, opposition en cours de vérification.

DROIT 6 — LE DROIT A LA PORTABILITE

Toute personne peut récupérer les données qu'elle a fournies a une organisation dans un format structure, couramment utilise et lisible par machine et les transférer a une autre organisation sans que l'organisation initiale puisse s'y opposer.

FOCUS AFRIQUE — La portabilite dans le secteur financier africain

Le droit a la portabilité est particulièrement pertinent dans le mobile money : un client devrait pouvoir récupérer son historique de transactions et le transférer vers un autre operateur. C'est un enjeu concurrentiel majeur en Afrique de l'Ouest ou plusieurs operateurs mobile money coexistent.

L'Open Banking qui impose techniquement la portabilité des données bancaires via des API est en émergence en Afrique (initiatives BCEAO sur la fintech) et crée une obligation pratique de mise en œuvre du droit a la portabilité.

DROIT 7 — LE DROIT D'OPPOSITION

Toute personne peut s'opposer, pour des raisons tenant à sa situation particulière, a un traitement fonde sur l'intérêt légitime ou la mission d'intérêt public. L'organisation doit cesser le traitement SAUF si elle démontre des motifs légitimement impérieux prépondérants.

Ce droit est ABSOLU et sans conditions pour le traitement à des fins de prospection commerciale directe une personne qui s'oppose au marketing direct doit être respectée immédiatement et sans conditions.

DROIT 8 — DROIT DE NE PAS FAIRE L'OBJET D'UNE DECISION AUTOMATISEE

Toute personne a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatise y compris le profilage produisant des effets juridiques la concernant ou l'affectant de manière significative similaire.

- **Exemples :** refus automatique de crédit par IA, tri automatique des candidatures, évaluation automatique des performances ;
- **Exception :** si la décision est nécessaire a la conclusion d'un contrat, autorisée par la loi ou basée sur le consentement explicite ;
- **Dans ces exceptions :** l'organisation doit proposer une intervention humaine, permettre à la personne d'exprimer son point de vue et de contester la décision.

DROIT 9 — DROIT DE RETIRER SON CONSENTEMENT

Si le traitement est fondé sur le consentement, la personne peut le retirer à tout moment aussi facilement qu'elle l'a donne. Le retrait ne remet pas en cause la licéité des traitements antérieurs.

DROIT 10 — DROIT DE DEPOSER UNE RECLAMATION

Toute personne a le droit de déposer une réclamation auprès de l'autorité de contrôle compétente si elle estime que le traitement la concernant viole les règles applicables. Ce droit est exerçable sans préjudice de tout recours juridictionnel.

◆ Gestion pratique des demandes de droits

L'organisation doit mettre en place un processus clair pour recevoir, traiter et répondre aux demandes d'exercice de droits. Ce processus doit être documente et teste.

Etape	Actions requises	Delai
Reception et verification	Identifier la personne (sans demander plus d'informations que nécessaire). Vérifier l'identité si la demande est sensible. Enregistrer la demande.	*J + 0*
Analyse et recherche	Localiser les données dans les systèmes. Evaluer si la demande est valide. Identifier les données concernées.	*J + 0 a J + 15*
Reponse a la personne	Fournir la réponse dans le délai légal. Si délai supplémentaire nécessaire (complexité), informer la personne avant la fin du premier mois.	*J + 30 (RGPD) — vérifier la loi locale*
Documentation	Conserver une trace de la demande et de la réponse. Utile en cas de litige ou contrôle de l'autorité.	*Pendant toute la durée légale applicable*

EXERCICE PRATIQUE — Exercice Simuler la gestion d'une demande de droit d'acces

Scenario : M. Amadou DIALLO, client de la BSF depuis 2018, vous envoie un email demandant : 'Je souhaite obtenir toutes les informations que vous avez sur moi, y compris mes transactions, mes evaluations de credit et les contacts avec votre service client.'

Questions a traiter :

1. Cette demande est-elle valide ? Quelles verifications d'identite effectuer ?
2. Dans quels systemes chercher les donnees ? (Listez au moins 5 systemes de la BSF)
3. Quelles donnees peuvent etre communiquees ? Y a-t-il des exceptions ?
4. Dans quel delai devez-vous repondre ? Que faire si vous avez besoin de plus de temps ?
5. Redigez l'email de reponse a M. DIALLO en langage clair et non juridique.

A RETENIR

- **10 droits fondamentaux :** Information, Accès, Rectification, Effacement, Limitation, Portabilité, Opposition, Pas de décision automatisée, Retrait consentement, Réclamation ;
- Le délai de réponse standard est d'un mois (RGPD) vérifier la loi nationale applicable ;
- Le droit à l'effacement n'est pas absolu des obligations de conservation légale (ex : données bancaires 10 ans) peuvent primer ;
- L'opposition au marketing direct est absolue et inconditionnelle à respecter immédiatement ;
- Les demandes de droits doivent être documentées preuve de la réponse en cas de contrôle de l'autorité.

PARTIE V —

MISE EN PRATIQUE

Privacy by Design, Transferts internationaux et Plan de mise en conformite

Chapitre 11 — Privacy by Design et Privacy by Default

DEFINITION — Privacy by Design

Approche selon laquelle la protection des données est intégrée des la CONCEPTION d'un système, d'un processus ou d'un produit, et non ajoutée a posteriori comme une contrainte. La protection des données est native, pas rétrofitée.

Le Privacy by Design, concept développé par Ann Cavoukian, commissaire a la vie privée de l'Ontario (Canada), est devenu une obligation légale avec le RGPD (article 25). Il s'articule autour de 7 principes fondateurs.

◆ Les 7 principes du Privacy by Design

1 — Proactif, non réactif	Anticiper les risques avant qu'ils ne surviennent. Ne pas attendre un incident pour protéger les données. Exemple : réaliser une EIPD avant de lancer un projet.
2 — Paramètre par défaut	Le niveau le plus protecteur de la vie privée doit être le réglage PAR DEFAUT, sans action de la personne. Exemple : les SMS marketing désactivent par défaut, les profils réseaux sociaux prives par défaut.
3 — Protection intégrée	La protection est intégrée dans la conception du système pas une couche ajoutée. Exemple : chiffrement des données intègre a l'architecture du Core Banking, pas installe apres.
4 — Fonctionnalité totale (zéro sum)	La protection des données n'est pas incompatible avec les fonctionnalités et l'innovation. Win-win, pas un compromis. Exemple : systèmes de paiement mobile sécurisés ET pratiques.
5 — Sécurité de bout en bout	Protection pendant TOUT le cycle de vie des données : collecte, traitement, stockage, transfert, archivage et suppression. Exemple : effacement sécurisé des données a l'expiration de la rétention.
6 — Visibilité et transparence	Les systèmes sont ouverts a l'examen : audits, certifications, politiques accessibles. Les personnes peuvent vérifier que leurs données sont protégées. Exemple : rapport de transparence annuel publie.
7 — Respect de la vie privée	Centrer la conception sur les intérêts et besoins de la personne concernée. Conserver les données exactes, accessibles et dans l'intérêt de la personne.

◆ Privacy by Default — le reglage le plus protecteur par defaut

Le Privacy by Default impose que, sans action spécifique de la personne, le traitement effectif des données personnelles soit limite au minimum nécessaire. En pratique :

- Seules les données strictement nécessaires a la finalité sont collectées par défaut (minimisation automatique) ;
- Les données ne sont pas conservées plus longtemps que nécessaire sans action active de la personne ;
- Les données ne sont pas rendues accessibles a un nombre indéterminé de tiers par défaut ;
- Les options de partage de publicité du profil, d'utilisation pour la publicité sont DESACTIVEES par défaut.

EXEMPLE — Privacy by Design dans le developpement d'une appli mobile money africaine

- **Des la conception :** L'equipe de developpement inclut un ***« security and privacy champion ».*** Une EIPD est realisee avant le debut du developpement. Les donnees a collecter sont listees et justifiees une a une (minimisation).
- **Architecture :** Separation des donnees d'identite et des donnees de transaction dans des bases differentes. Chiffrement de bout en bout des communications. Tokenisation des numeros de cartes bancaires.
- **Parametre par defaut :** Historique des transactions visible uniquement 3 mois par defaut. Notifications marketing desactivees par defaut. Partage des donnees avec des partenaires optionnel et opt-in.
- **Cycle de vie :** Procedure automatique d'effacement des donnees inactives apres 5 ans. Logs d'acces conserves 12 mois puis anonymises. Sauvegarde chiffree avec duree de retention definie.

Chapitre 12 — Transferts internationaux de donnees

Le transfert de donnees personnelles vers un pays tiers (hors UE pour le RGPD, hors territoire national pour les lois africaines) n'est licite que si des garanties appropriees sont en place pour assurer un niveau de protection equivalent. Ce principe protege les personnes contre les transferts vers des pays a faible niveau de protection.

◆ Les mecanismes de transfert

Mecanisme	Description	Conditions d'utilisation
Decision d'adequation	Le pays destinataire est reconnu par l'autorite competente comme offrant un niveau de protection equivalent. Aucune autre garantie n'est requise.	*Verifier si le pays de destination fait l'objet d'une decision d'adequation (ex : pays europeens, Canada, Japon pour le RGPD)*
Clauses contractuelles types (CCT)	Contrat type pre-approuve par l'autorite de controle, signé entre l'exportateur et l'importateur de donnees.	*Disponibles pour responsable → responsable et responsable → sous-traitant. Doit etre complete par une evaluation du risque pays.*
Regles d'entreprise contraignantes (BCR)	Politique interne de protection des donnees approuvee par les autorites, applicable dans tous les pays du groupe multinational.	*Reservees aux groupes multinationaux processus d'approbation long et complexe*
Codes de conduite et certifications	Adherer a un code de conduite approuve ou obtenir une certification reconnue par les autorites.	*En developpement rares codes africains approuves pour l'instant*
Exceptions specifiques	Consentement explicite, execution d'un contrat, interet public important, exercice de droits en justice...	*Utilisation limitee et justifiee ne peuvent pas etre la base habituelle des transferts*

◆ Les transferts africains — specificites

Pour les organisations africaines, les transferts internationaux sont tres frequents :

- Utilisation de services cloud (AWS, Azure, Google Cloud) dont les serveurs sont principalement en Europe ou aux Etats-Unis ;
- Utilisation de logiciels SaaS (Microsoft 365, Salesforce, Temenos T24 en cloud) ;
- Transferts via SWIFT vers des banques correspondantes dans le monde entier ;
- Partage de donnees avec des organismes internationaux (FMI, Banque Mondiale) ;
- Sous-traitance informatique vers des ESN exterieures au territoire national.

FOCUS AFRIQUE — Comment conformer les transferts africains ?

Etape 1 : Cartographier tous les transferts (dans le registre des traitements). Identifier les pays de destination.

Etape 2 : Evaluer si le pays de destination dispose d'un niveau de protection adequat selon la loi applicable.

Etape 3 : Si pas adequat, mettre en place le mecanisme approprie (CCT dans les contrats avec les prestataires cloud, evaluation des fournisseurs...).

Etape 4 : Inclure dans les politiques de confidentialite une section sur les transferts et les garanties mises en oeuvre.

Conseil pratique : inclure systematiquement des clauses de protection des donnees dans TOUS les contrats avec des prestataires IT etrangers c'est le premier reflexe du DPO africain.

◆ Plan de mise en conformite — feuille de route

Pour une organisation africaine souhaitant se mettre en conformite avec la protection des donnees, voici la feuille de route recommandee en 6 phases :

Phase	Actions prioritaires	Duree type
Phase 1 — Etat des lieux	Cartographier tous les traitements. Identifier les bases legales existantes. Evaluer les risques principaux. Nommer (ou identifier) un DPO.	*4-8 semaines*
Phase 2 — Documentation	Construire ou mettre a jour le registre des traitements. Rediger / mettre a jour les politiques de confidentialite. Documenter les bases legales.	*8-12 semaines*
Phase 3 — Droits des personnes	Mettre en place le processus de gestion des demandes de droits. Tester les procedures. Former les equipes en contact avec les clients.	*4-6 semaines*
Phase 4 — Securite et EIPD	Aligner les mesures de securite sur les exigences de la loi. Realiser les EIPD pour les traitements a risque. Mettre en place la procedure de gestion des violations.	*8-16 semaines*
Phase 5 — Formation et culture	Sensibiliser l'ensemble du personnel. Former specifiquement les equipes IT, RH, marketing et juridique. Integrer la protection des donnees dans les processus RH (onboarding, depart).	*Continu*
Phase 6 — Maintien et amelioration	Revue annuelle du registre et des EIPD. Veille reglementaire. Mise a jour suite aux changements. Audits internes periodiques.	*Continu — annuel minimum*

A RETENIR

- **Privacy by Design :** integrer la protection des donnees DES LA CONCEPTION, pas apres. C'est une obligation legale (RGPD art. 25)
- **Privacy by Default :** le niveau de protection le plus eleve est le reglage par defaut, sans action de l'utilisateur
- **Transferts internationaux :** toujours verifier si le pays destinataire est **« adequat »** ou mettre en place une garantie appropriee (CCT)
- La mise en conformite est un programme de 12-18 mois minimum pour une organisation de taille moyenne
- La conformite en protection des donnees n'est jamais acquise c'est un processus continu d'amelioration

QUIZ D'AUTO-EVALUATION — 15 QCM

Protection des donnees personnelles

Repondez avant de consulter la correction. Objectif : 12/15 minimum.

Q1. Parmi les donnees suivantes, laquelle n'est PAS une donnee personnelle ?

- **A.** L'adresse email professionnelle d'un employe
- **B.** Le numero de plaque d'immatriculation d'un vehicule
- **C.** Les statistiques de ventes aggregees sans identification individuelle
- **D.** Le numero de compte bancaire d'un client

Reponse : C — Statistiques aggregees sans identification

Les statistiques aggregees et anonymisees irreversiblement ne sont pas des donnees personnelles car elles ne permettent pas d'identifier une personne physique. Les trois autres options permettent une identification directe ou indirecte.

Q2. Qu'est-ce que le principe de minimisation des donnees impose ?

- **A.** De minimiser le nombre de systemes qui traitent les donnees
- **B.** De ne collecter que les donnees adequates, pertinentes et strictement necessaires a la finalite
- **C.** De reduire le budget alloue a la gestion des donnees
- **D.** De limiter le nombre de personnes ayant acces aux donnees

Reponse : B — Ne collecter que ce qui est adequat, pertinent et necessaire

Le principe de minimisation impose de ne pas collecter de donnees 'au cas ou' ou 'parce que c'est possible'. Chaque donnee collectee doit etre directement necessaire a la finalite declaree du traitement.

Q3. Un consentement valide doit etre :

- **A.** Obtenu par email uniquement
- **B.** Libre, specifique, eclaire, univoque et revocable
- **C.** Donne une seule fois pour toutes les finalites
- **D.** Oral ou ecrit au choix de l'organisation

Reponse : B — Libre, specifique, eclaire, univoque et revocable

Le RGPD et les lois africaines inspirees exigent que le consentement soit : libre (pas de consequence si refus), specifique (par finalite), eclaire (personne comprend), univoque (action positive deliberee) et revocable a tout moment.

Q4. Dans quel delai maximum une organisation doit-elle notifier une violation de donnees a l'autorite de controle (RGPD) ?

- **A.** 24 heures
- **B.** 48 heures
- **C.** 72 heures
- **D.** 7 jours

Reponse : C — 72 heures

Le RGPD impose une notification a l'autorite de controle dans les 72 heures suivant la prise de connaissance d'une violation, si elle est susceptible d'engendrer un risque pour les droits et libertes. Ce delai est repris par les lois africaines modernes (Niger, Togo).

Q5. Qu'est-ce que le 'droit a l'oubli' (droit a l'effacement) permet ?

- **A.** D'effacer automatiquement toutes ses donnees apres 2 ans
- **B.** De demander la suppression de ses donnees dans certaines conditions specifiques
- **C.** D'effacer son historique de navigation sur internet
- **D.** D'interdire toute publication de son nom sur internet

Reponse : B — Demander la suppression dans certaines conditions specifiques

Le droit a l'effacement n'est pas absolu. Il s'applique notamment quand les donnees ne sont plus necessaires, quand le consentement est retire, ou quand le traitement est illicite. Des obligations de conservation legale (comptables, fiscales) peuvent primer.

Q6. Qu'est-ce que la 'pseudonymisation' ?

- **A.** La suppression definitive et irreversible de toute donnee d'identification
- **B.** La substitution d'un identifiant direct par un code, tout en conservant la possibilite de re-identification
- **C.** Le changement d'identite numerique d'une personne
- **D.** La cryptage des donnees personnelles avec une cle publique

Reponse : B — Substitution par un code avec possibilite de re-identification

La pseudonymisation remplace les identifiants directs (nom, prenom) par un code, mais la re-identification reste possible avec une cle de correspondance. Les donnees pseudonymisees restent des donnees personnelles, contrairement aux donnees anonymisees irreversiblement.

Q7. Quand une EIPD (Etude d'Impact sur la Protection des Donnees) est-elle obligatoire ?

- **A.** Pour tout nouveau traitement de donnees personnelles
- **B.** Uniquement pour les traitements de donnees medicales
- **C.** Lorsqu'un traitement est susceptible d'engendrer un risque eleve pour les droits et libertes
- **D.** Tous les 3 ans pour tous les traitements existants

Reponse : C — Traitement susceptible d'engendrer un risque eleve

L'EIPD est obligatoire pour les traitements a risque eleve : evaluation/scoring systematique, decisions automatisees significatives, surveillance a grande echelle, donnees sensibles a grande echelle, croisement de donnees, nouvelles technologies...

Q8. Parmi les bases legales suivantes, laquelle est INCORRECTE (n'existe pas dans le RGPD) ?

A. Le consentement
B. L'interet commercial de l'organisation
C. L'obligation legale
D. L'interet legitime

Reponse : B — L'interet commercial de l'organisation

Il n'existe pas de base legale 'interet commercial' dans le RGPD ou les lois africaines modernes. Les 6 bases legales valides sont : consentement, contrat, obligation legale, interet vital, mission d'interet public, interet legitime (qui suppose un test de balance des interets, pas un simple interet commercial).

Q9. Qu'est-ce que le 'Privacy by Default' impose ?

A. Que toutes les donnees soient chiffrees par defaut
B. Que le niveau de protection le plus eleve soit le reglage par defaut, sans action de l'utilisateur
C. Que les donnees soient supprimees apres 6 mois par defaut
D. Que le DPO soit informe par defaut de tous les traitements

Reponse : B — Niveau de protection le plus eleve par defaut sans action de l'utilisateur

Le Privacy by Default impose que, sans action de l'utilisateur, les donnees traitees soient limitees au minimum necessaire, non rendues accessibles a des tiers par defaut, et que les options de partage soient desactivees par defaut.

Q10. Quelle loi africaine est consideree comme la plus proche du RGPD europeen dans la region UEMOA ?

A. Loi senegalaise de 2008
B. Loi burkinabe de 2004
C. Loi togolaise de 2019
D. Loi ivoirienne de 2013

Reponse : C — Loi togolaise n°2019-014

La loi togolaise de 2019 est la plus recente et la plus proche du RGPD en zone UEMOA. Elle integre le DPO, l'EIPD, la notification en 72h, la portabilite des donnees et les sanctions renforcees elements absents des lois plus anciennes comme la loi senegalaise de 2008.

Q11. Le DPO (Delegue a la Protection des Donnees) peut-il etre sanctionne ou revoque pour avoir signale une non-conformite ?

A. Oui, si la direction le décide
B. Non, le DPO bénéficie d'une indépendance et d'une protection contre les représailles
C. Oui, si l'actionnaire principal l'exige
D. Cela dépend du pays et de la taille de l'organisation

Réponse : B — Non, le DPO est protège contre les représailles

Le DPO doit exercer ses fonctions en toute indépendance. Il ne peut pas recevoir d'instructions sur la manière d'exercer ses missions et ne peut pas être pénalisé ou révoque pour avoir accompli sa mission de signalement. Cette protection est fondamentale pour l'efficacité du dispositif.

Q12. Qu'est-ce que le droit a la portabilite permet ?

A. De deplacer physiquement les serveurs contenant ses donnees
B. De recuperer ses donnees dans un format lisible par machine et de les transferer a une autre organisation
C. D'acceder a ses donnees depuis n'importe quel pays
D. De dupliquer ses donnees sur plusieurs plateformes simultanement

Reponse : B — Recuperer ses donnees et les transferer a une autre organisation

Le droit a la portabilite permet de recevoir ses donnees (fournies a l'organisation) dans un format structure, lisible par machine, et de les transferer a un concurrent ou une autre organisation. C'est un droit clé pour la concurrence dans le numerique.

Q13. Pour qu'un transfert de donnees vers un pays tiers soit licite selon le RGPD, quelle condition doit etre remplie en premier ?

A. L'accord du PDG de l'organisation
B. L'existence d'une decision d'adequation ou de garanties appropriees (CCT, BCR)
C. L'approbation de la chambre de commerce locale
D. La duree du transfert doit etre inferieure a 30 jours

Reponse : B — Decision d'adequation ou garanties appropriees

Tout transfert vers un pays tiers doit s'appuyer sur un mecanisme de transfert valide : decision d'adequation (le pays offre une protection equivalente), clauses contractuelles types, regles d'entreprise contraignantes, ou une des exceptions specifiques limitees.

Q14. Quelle est la difference entre un responsable du traitement et un sous-traitant ?

A. Le responsable traite plus de donnees que le sous-traitant
B. Le responsable determine les finalites et moyens du traitement ; le sous-traitant traite pour le compte du responsable sur ses instructions
C. Le sous-traitant est toujours un prestataire externe ; le responsable est toujours interne
D. Il n'y a aucune difference pratique entre les deux

Reponse : B — Responsable determine les finalites ; sous-traitant execute sur instructions

Le responsable du traitement decide du pourquoi et du comment du traitement. Le sous-traitant execute le traitement pour le compte du responsable, uniquement selon ses instructions. Cette distinction determine les obligations et responsabilites de chacun.

Q15. Une donnee biometrique (empreinte digitale pour ouverture de compte mobile money) est :

A. Une donnee personnelle ordinaire
B. Une donnee sensible necessitant une protection renforcee et une base legale specifique
C. Une donnee anonyme car elle est codee en base de donnees
D. Une donnee qui n'est pas encore reglementee en Afrique

Reponse : B — Donnee sensible necessitant protection renforcee et base legale specifique

Les donnees biometriques aux fins d'identification unique d'une personne physique sont des donnees de categorie speciale (sensibles) selon le RGPD et les lois africaines modernes. Leur traitement est en principe interdit sauf exceptions strictes avec base legale specifique et mesures de securite renforcees.

POINTS CLES — Scoring du quiz

- 15/15 : Excellent — vous etes pret(e) pour une specialisation DPO africain
- 12-14/15 : Tres bien — revoyez les questions manquees et procedez au cas pratique
- 9-11/15 : Bien — relecture recommandee des chapitres correspondant a vos erreurs
- Moins de 9/15 : Relecture complete du cours et session avec votre mentor recommandee

LEXIQUE — PROTECTION DES DONNEES

Termes essentiels du professionnel DPO et GRC

Accountability	Principe de responsabilite l'organisation doit non seulement respecter les regles mais prouver qu'elle les respecte
Anonymisation	Transformation irreversible des donnees rendant l'identification d'une personne techniquement impossible sort les donnees du champ de la reglementation
Autorite de controle	Organisme independant charge de veiller a l'application de la loi de protection des donnees (CDP, ANPDP, ARDP, ARTCI...)
Base legale	Fondement juridique qui rend licite le traitement de donnees personnelles. Les 6 bases : consentement, contrat, obligation legale, interet vital, interet public, interet legitime
BCR (Binding Corporate Rules)	Regles d'entreprise contraignantes approuvees par les autorites pour encadrer les transferts intra-groupes internationaux
CCT (Clauses Contractuelles Types)	Contrats types approuves pour encadrer les transferts de donnees personnelles vers des pays tiers sans decision d'adequation
Consentement	Accord libre, specifique, eclaire, univoque et revocable d'une personne au traitement de ses donnees
Convention de Malabo	Convention de l'Union Africaine (2014) sur la cybersecurite et la protection des donnees personnelles pas encore en vigueur
Decision d'adequation	Decision par laquelle une autorite reconnait qu'un pays tiers offre un niveau de protection equivalent permet les transferts sans garanties supplementaires
Donnee personnelle	Toute information permettant d'identifier directement ou indirectement une personne physique
Donnee sensible	Donnee de categorie speciale dont le traitement est en principe interdit : biometrie, sante, origine ethnique, opinions politiques, vie sexuelle...
DPO (Delegue a la Protection des Donnees)	Expert independant charge de superviser la conformite de l'organisation avec les lois de protection des donnees
Droit a l'oubli	Droit a l'effacement de ses donnees dans certaines conditions pas absolu peut etre prime par des obligations de conservation
Droit de portabilite	Droit de recuperer ses donnees dans un format lisible par machine et de les transferer a une autre organisation
EIPD / DPIA	Etude d'Impact relative a la Protection des Donnees analyse prospective obligatoire pour les traitements a risque eleve
Finalite	Objectif declare et legitime pour lequel des donnees personnelles sont collectees et traitees
Interet legitime	Base legale permettant le traitement si l'interet de l'organisation prime sur les droits des personnes necessite un test de balance

Minimisation	Principe imposant de ne collecter que les donnees adequates, pertinentes et strictement necessaires
Notification de violation	Obligation d'informer l'autorite de controle dans les 72h apres decouverte d'une violation de donnees a risque
Open Banking	Initiative permettant aux clients de partager leurs donnees bancaires avec des tiers via des API lie au droit de portabilite
Politique de confidentialite	Document informant les personnes sur les traitements de leurs donnees materialise le droit a l'information
Privacy by Default	Le reglage le plus protecteur de la vie privee est actif par defaut sans action de l'utilisateur
Privacy by Design	Integration de la protection des donnees des la conception d'un systeme ou produit pas en retrofit
Profilage	Toute forme de traitement automatise consistant a utiliser des donnees pour evaluer, analyser ou predire des aspects d'une personne
Pseudonymisation	Traitement qui ne permet plus d'attribuer des donnees a une personne sans information supplementaire conservee separement
RGPD	Reglement General sur la Protection des Donnees (UE) 2016/679 reference mondiale, extraterritorial pour les organisations africaines
Registre des traitements	Document interne listant toutes les activites de traitement de donnees obligatoire sous le RGPD et lois africaines modernes
Responsable du traitement	Personne ou organisme qui determine les finalites et les moyens du traitement de donnees personnelles
Retention (duree de)	Duree pendant laquelle les donnees peuvent etre conservees au-dela, effacement ou anonymisation obligatoires
Sous-traitant	Personne ou organisme qui traite des donnees personnelles pour le compte du responsable du traitement, sur ses instructions
Traitement	Toute operation appliquee a des donnees personnelles : collecte, enregistrement, stockage, consultation, transmission, effacement...

REFERENCES ET RESSOURCES

◆ Textes fondamentaux

- RGPD — Reglement UE 2016/679 — eur-lex.europa.eu
- Convention 108+ du Conseil de l'Europe — coe.int/fr/web/data-protection
- Convention de Malabo — Union Africaine (2014) — au.int
- Acte Additionnel CEDEAO A/SA.1/01/10 sur la protection des donnees — ecowas.int

◆ Lois africaines (liens officiels)

- Senegal — Loi n°2008-12 — jo.gouv.sn • Autorite : cdp.sn
- Niger — Loi n°2020-037 — Autorite : anpdp.gouv.ne
- Togo — Loi n°2019-014 — Autorite : ardp.tg
- Cote d'Ivoire — Loi n°2013-450 — Autorite : artci.ci
- Burkina Faso — Loi n°010-2004 — Autorite : cil.gov.bf
- Maroc — Loi 09-08 — Autorite : cndp.ma

◆ Ressources pedagogiques

- CNIL (France) — Guides pratiques gratuits : cnil.fr/fr/professionnels reference mondiale francophone
- IAPP — International Association of Privacy Professionals — iapp.org — certifications CIPP, CIPM
- ACRC — Africa Cybersecurity Resource Centre — acrc-africa.org — formations AFP
- ANSSI — EBIOS RM et guides securite — ssi.gouv.fr
- Future of Privacy Forum — fpf.org — ressources sur les technologies emergentes

◆ Certifications professionnelles DPO

CIPP/E — IAPP	Certified Information Privacy Professional / Europe — reference mondiale pour les DPO RGPD
CIPP/A — IAPP	Certified Information Privacy Professional / Asia — couvre les lois Asie-Pacifique dont l'Afrique du Sud (POPIA)
CDPO — PECB	Certified Data Protection Officer — specialisation DPO, disponible en francais
AFP-Gouv — ACRC	Africa Financial Professional Governance — certification panafricaine GRC incluant la protection des donnees
DPO-Afrique (en developpement)	Certification specialisee DPO pour les legislations africaines — initiative APSI-NE et partenaires

APSI-NE x ACRC — Programme d'Excellence en Cybersecurite — Cohorte 2026

Document pedagogique confidentiel — Usage formation exclusif