La Protection des données au cœur des enjeux gouvernementaux au Cameroun :

Stratégies et Responsabilités

Prof Jean Louis Ebongue Fendji
Université de Ngaoundéré

Who is who?

Courte présentation de chacun:

- Nom et prénom
- Administration/Service
- Attentes

AGENDA

01 **Introduction**

02 **Contexte et Enjeux de la Protection des Données**

03 **Cadre Juridique et Réglementaire**

04 **Stratégies de Protection des Données**

05 **Responsabilités et Rôles**

06 **Conclusion**

01

Introduction

Introduction 1/3

Pourquoi la protection des données est cruciale ?

- Transformation numérique et *donnéesfication* (datafication) : multiplication de la quantité de données collectées et traitées, y compris par les gouvernements.
- Conséquence: Risque de violations de la vie privée, mise en péril de la sécurité nationale, érosion de la confiance publique.
- Quelques récents incidents :
  - Fuite de documents administratifs avec saut « Confidentiel », « Secret », « Secret Défense ». Documents de la présidence, des ministères, des tribunaux…
  - Fuite des épreuves d'examen

Introduction 2/3

Enjeux pour le Gouvernement et les Ministères

- Le rôle central du gouvernement dans la collecte, la gestion et la protection des données:
  - Des informations personnelles des citoyens à des données critiques pour la sécurité nationale.
  - Responsabilité accrue en matière de protection des données, par rapport aux autres types d'organisations.
- Risques spécifiques aux données gouvernementales:
  - Données de sécurité et de défense, Données sur les infrastructures critiques, Données relatives aux affaires intérieures et à la gouvernance,
  - Données personnelles et d'état civil, Santé, financières et fiscales
- Importance de maintenir la confiance du public à travers des pratiques robustes de protection des données

Introduction 3/3

Objectifs

- Présenter un aperçu général de la protection des données.
- Sensibiliser sur les responsabilités des différents acteurs dans la gestion et la protection des données.
- Mettre en lumière les bonnes pratiques et les stratégies pour renforcer la sécurité des données au sein des institutions.

02

Contexte et Enjeux de la Protection des Données

Contexte et Importance de la Protection des Données 1/6

Transformation Numérique

- La transition vers une société numérique a transformé la manière dont les données sont collectées, stockées et partagées.
  - Utilisation accrue de services en ligne, de systèmes de gestion électroniques et de plateformes de communication numérique.
  - Explosion de la quantité de données produites, notamment les données personnelles et sensibles, ce qui rend leur protection plus complexe et plus critique.
- Risque de Centralisation des Données
  - Système central peut augmenter les risques de violation de données, car un incident pourrait exposer une grande quantité d'informations sensibles à la fois.

Contexte et Importance de la Protection des Données 2/6

Conséquences des Violations de Données

- Impact sur les individus.
  - Conséquences directes des violations de données pour les individus, notamment le vol d'identité, la fraude, et les atteintes à la vie privée.
  - Une perte de confiance du public dans les institutions gouvernementales, réduisant ainsi l'efficacité de leurs services.
- Impact sur les Organisations
  - Dommages irréparables à la réputation d'une organisation, ce qui peut compromettre la crédibilité et l'autorité du gouvernement.

Contexte et Importance de la Protection des Données 3/6

Données Sensibles vs Personnelles

- Données personnelles: informations comme les noms, num Tél, num immatriculation unique …
- Données sensibles: informations de santé, des données financières, ou des affiliations politiques…
- Protection des Données Sensibles
  - Données sensibles nécessitent des niveaux de protection plus élevés, y compris des mesures comme le cryptage, des accès restreints, et des audits réguliers.
  - Conséquences en termes de sécurité publique ou de souveraineté nationale

Contexte et Importance de la Protection des Données 4/6

Enjeux pour les Gouvernements et les Ministères

- Rôle du Gouvernement: responsabilité unique en matière de protection des données en raison de la nature et de l'étendue des informations qu'il gèrent.
  - Données des citoyens: informations fiscales, les dossiers médicaux, les données d'immigration, et les statistiques de recensement
  - Informations critiques liées à la sécurité nationale et à la gouvernance.
- Nécessite le respect des droits des citoyens en matière de vie privée, tout en assurant que les données sont utilisées de manière sécurisée et éthique.

Contexte et Importance de la Protection des Données 5/6

Enjeux pour les Gouvernements et les Ministères

- Risques spécifiques au Gouvernement:
  - Cyberattaques et Espionnage: cible privilégiée pour les cyberattaques, en raison de la valeur des informations qu'il détient. Les attaquants peuvent être motivés par des raisons financières, politiques ou même idéologiques
  - Fuites d'Informations Confidentielles: négligence, erreur humaine, ou règlement de compte. Par exemple: envoi accidentel d'un courriel contenant des informations sensibles à un destinataire incorrect peut entraîner des conséquences graves. Ou le partage d'une information sensible par WhatsApp peut devenir viral.

Contexte et Importance de la Protection des Données 6/6

Enjeux pour les Gouvernements et les Ministères

- Maintien de l'ordre et de la Confiance Publique :
  - Les citoyens doivent être convaincus que leurs données sont protégées et utilisées de manière appropriée. Si les données sensibles ne sont pas protégées, à plus forte raison les données personnelles.
  - Un gouvernement qui ne protège pas correctement les données de ses citoyens risque de perdre leur confiance, ce qui peut avoir des répercussions sur l'engagement civique et la coopération.
- Besoin de transparence et communication:
  - Communication claire des politiques de protection des données, ainsi que la transparence sur les incidents de sécurité et les mesures prises pour y remédier

03

Cadre Juridique et Réglementaire

Cadre Juridique et Réglementaire

Réglementation Nationale

- Pas de réglementation sur la protection des données, mais un avant projet
- Dispositions dans certains textes : la loi sur la cybersécurité ; la loi sur les communications électroniques; la loi sur le commerce électronique; la loi sur la protection du consommateur; la loi sur les exigences d'identification; le décret sur la protection des consommateurs en matière de communications électroniques, la réforme de l'article 241 du Code pénal
- La Loi N°2024/001 du 24 juillet 2024 régissant les archives au Cameroun

Réglementation Internationale

- La Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles du 27 juin 2014 (« la Convention de Malabo ») a été signée par le Cameroun le 12 août 2021 (ratification attendue).
- Le règlement général sur la protection des données (Règlement (UE) 2016/679) (« RGPD »)

CONVENTION DE MALABO

Principes de Base en Matière de Protection des Données

la légalité, la transparence, la finalité légitime, la proportionnalité, la pertinence, la confidentialité, et la sécurité des données. Art. 13-14

Droits des Personnes Concernées

Le droit à l'information, le droit d'accès, le droit de rectification, et le droit d'opposition au traitement de leurs données. Art. 16-18

Obligations des Responsables du Traitement

La sécurité des données à caractère personnel contre toute forme de perte, d'accès non autorisé, de modification ou de divulgation. Art. 10-14

Autorités Nationales de Protection des Données

Désigner une autorité nationale indépendante chargée de la protection des données à caractère personnel. Art. 11-12
Etablir des mesures législatives pour permettre aux autorités de protection des données d'imposer ces sanctions et d'assurer la conformité. Art. 23-24

Protection des Données Sensibles

Restrictions spécifiques sur le traitement des données sensible (origine raciale ou ethnique, opinions politiques, croyances religieuses, données biométriques et les informations sur la santé. Art. 15

Promotion de la Culture de la Protection des Données

Sensibiliser le public à l'importance de la protection des données à caractère personnel et à promouvoir une culture de respect de la vie privée. Art. 9-10

Avant projet de loi sur la PD

Faiblesse des mécanismes de consentement

Consentement libre, éclairé, spécifique et univoque. Mais manque de détails sur la manière dont ce consentement doit être obtenu (surtout technos complexes). RGPD, standards plus stricts.

Protection insuffisante des données sensibles

Art.17 interdit traitement de certaines catégories de données sensibles, Mais prévoit des exceptions qui pourraient être exploitées pour contourner cette interdiction. (intérêt public

Absence de droits clairement définis pour les individus

Mention de certains droits des personnes concernées (droit à l'accès, à la rectification, et à l'effacement des données). Mais manque de détails sur l'application de ces droits (portabilité des données

Indépendance limitée de l'Autorité de Protection

Instituée auprès du Premier ministre. Pourrait poser des problèmes d'indépendance. Bien que décrite comme bénéficiant d'une autonomie de gestion et financière, sa composition, qui inclut des membres nommés par des autorités politiques, pourrait influencer son impartialité.

Encadrement faible des transferts internationaux données

Permet le transfert de données à caractère personnel vers des pays étrangers ou des organisations internationales sous certaines conditions, mais il n'établit pas de mécanisme clair pour l'évaluation des protections adéquates dans ces pays.

Sanctions et mécanismes d'application

Prévoit des sanctions administratives et pénales pour les violations des dispositions, mais ces sanctions peuvent être jugées insuffisantes pour dissuader les grandes entreprises ou les administrations publiques de commettre des infractions

Loi sur les archives au Cameroun

Archivage électronique

Inclut l'archivage électronique: identification, collecte, classement et conservation des informations sur des supports électroniques pour une consultation ultérieure. Implique gestion rigoureuse des données pour assurer leur protection. Art 2. Def 3

Confidentialité des archives

Les archives contenant des informations relevant du secret professionnel ou des intérêts stratégiques de l'État peuvent être classées confidentielles. Cela protège les données personnelles sensibles contre toute divulgation non autorisée. Art 16

Données

Représentation de faits, indications enregistrées, chiffres, énoncés et caractères sous forme brute, ou de notions sous une forme traitable par un ordinateur. Définition cruciale pour traitement et protection des données personnelles contenues dans les archives. Art 2 Def 21

Accès aux données personnelles archivées

Toute personne a le droit d'accéder aux données personnelles qui la concernent, archivées par les institutions publiques, sous réserve des restrictions légales. Ce droit est également étendu aux ayants droit après le décès de l'intéressé, assurant ainsi la protection et l'accès aux informations personnelles. Art 25

Intégrité et sécurité des documents électroniques

Impose aux organismes publics et privés de garantir l'intégrité, l'authenticité, l'accessibilité, le respect des délais de protection, et la sécurité des documents électroniques, y compris les données personnelles. Art 19.

Sanctions et mécanismes d'application

Sanctions pénales pour la destruction, l'altération, ou le détournement de documents d'archives, y compris les données personnelles. Ces sanctions visent à protéger l'intégrité des données et à prévenir les abus. Art 42

04

Stratégies de Protection des Données

Stratégies de Protection des Données

Politiques et Procédures Internes

Développement de Politiques de Protection des Données

- Élaborer des politiques claires : aborder tous les aspects de la gestion des données, de la collecte à l'archivage/destruction.
- Adapter les politiques aux spécificités de chaque institution, en tenant compte des types de données traitées, de la sensibilité des informations, et des risques spécifiques auxquels l'institution est exposée.
- Inclure les principes fondamentaux : minimisation des données (ne collecter que ce qui est nécessaire), la transparence (informer les citoyens sur l'utilisation de leurs données), et la sécurité (protéger les données contre les accès non autorisés).
- Etablir des politiques de conservation des données, précisant combien de temps les données doivent être conservées et sous quelles conditions elles doivent être détruites.

Stratégies de Protection des Données

Politiques et Procédures Internes

Mise en Œuvre des Procédures de Gestion des Données

- Définir les procédures de collecte des données qui doivent être mises en place pour garantir que les données sont collectées de manière légale, transparente, et dans le respect de la vie privée des individus. Cela inclut l'obtention du consentement lorsque nécessaire.
- Décrire les procédures de traitement des données, en mettant l'accent sur l'importance de limiter l'accès aux données aux seules personnes autorisées et de s'assurer que les données sont traitées de manière sécurisée tout au long de leur cycle de vie.
- Surveiller régulièrement l'application des politiques et procédures pour s'assurer qu'elles sont respectées. Peut inclure des audits internes réguliers, des contrôles d'accès, et des revues de conformité.
- Documenter ces audits et de prendre des mesures correctives en cas de non-conformité, afin d'améliorer en continu les processus de gestion des données.

Stratégies de Protection des Données

Politiques et Procédures Internes

Planification de la Continuité des Activités

- Intégrer la gestion des risques dans les politiques de protection des données. Cela implique:
  - Identifier les risques potentiels (par exemple, les cyberattaques, les catastrophes naturelles) et
  - Mettre en place des plans pour minimiser leur impact sur la sécurité des données..
- Penser les plans de continuité des activités et des plans de reprise après sinistre. Doit inclure:
  - Des stratégies spécifiques pour protéger les données en cas d'incident majeur, comme la mise en place de sauvegardes régulières et la redondance des systèmes critiques.

Stratégies de Protection des Données

Technologies de Protection des Données

Utilisation de la Cryptographie

- Chiffrement des données, à la fois en transit et au repos, est l'une des meilleures défenses contre les accès non autorisés et les violations de données.
- Utilisé pour renforcer les mécanismes d'authentification, (l'utilisation de certificats numériques et de signatures électroniques) pour garantir l'intégrité des données et l'identité des utilisateurs.
- Systèmes de gestion des accès basés sur les rôles: accès limité en fonction des responsabilités.

Pare-feux, Systèmes de Détection d'Intrusion, Sécurité des Endpoints

- Maintien des pare-feux à jour avec les dernières règles de sécurité
- IDS qui surveillent les réseaux pour détecter les activités suspectes ou malveillantes
- Mise en place de politiques de sécurité sur tous les appareils utilisés par les employés, comme l'application de correctifs de sécurité réguliers, la limitation des logiciels installés, et la surveillance des activités des utilisateurs.

Stratégies de Protection des Données

Surveillance et Détection des Incidents de Sécurité

Surveillance Continue des Systèmes

- Surveillance continue des systèmes pour détecter rapidement les incidents de sécurité. Inclut la surveillance du réseau, des BDs, et des systèmes d'exploitation pour repérer les activités suspectes. Utilisation de tableaux de bord de sécurité (SIEM - Security Information and Event Management)
- Configuration des alertes automatiques pour signaler immédiatement les comportements anormaux ou les violations potentielles de sécurité.
- Collecte systématique des logs (journaux d'événements) pour retracer les actions et les événements qui se produisent au sein des systèmes informatiques. L'analyse régulière peut aider à détecter des anomalies, identifier des menaces, et reconstituer les événements en cas d'incident de sécurité.
- Audits de sécurité réguliers, inclure des tests d'intrusion pour identifier les vulnérabilités potentielles avant que des attaquants ne les exploitent.

Stratégies de Protection des Données

Surveillance et Détection des Incidents de Sécurité

Réponse aux Incidents de Sécurité

- Disposer d'un processus clair et documenté pour répondre aux incidents de sécurité. Ce processus doit inclure des étapes pour détecter, contenir, éradiquer, et récupérer les systèmes affectés.
- Former les équipes de réponse aux incidents pour qu'elles soient prêtes à réagir rapidement et efficacement en cas de violation de sécurité.

Analyse Post-incident

- Réaliser une analyse post-incident pour comprendre comment et pourquoi l'incident s'est produit. Cette analyse doit identifier les faiblesses qui ont permis l'incident, et proposer des mesures pour éviter qu'il ne se reproduise.
- Mettre à jour les politiques de sécurité et de former le personnel suite à un incident pour renforcer la résilience de l'organisation.

Stratégies de Protection des Données

Formation et Sensibilisation

Formation Continue du Personnel

- La formation continue des employés est cruciale pour maintenir une culture de sécurité forte au sein des ministères. Les programmes de formation doivent couvrir les meilleures pratiques en matière de gestion des données, les obligations légales, et les protocoles de sécurité
- Les formations doivent être adaptées aux différents rôles au sein de l'organisation, avec des sessions spécifiques pour les gestionnaires de données, les équipes IT, et les utilisateurs finaux.
- Les formations spécialisées pour les responsables de la protection des données, les administrateurs système, et les équipes de réponse aux incidents. Doit inclure des aspects techniques avancés ainsi que des simulations d'incidents pour préparer les équipes à des scénarios réels.
- Rester à jour avec les nouvelles menaces et les évolutions technologiques, en proposant des formations continues et des certifications pour le personnel clé.

Stratégies de Protection des Données

Formation et Sensibilisation

Campagnes de Sensibilisation

- Sensibilisation pour rappeler régulièrement aux employés les risques liés à la gestion des données et l'importance de respecter les politiques de sécurité. Peut inclure des bulletins d'information, des ateliers interactifs, et des rappels réguliers sur les bonnes pratiques.
- Sensibilisation spécifique sur des sujets comme le phishing, l'utilisation sécurisée des mots de passe, et la gestion des accès aux systèmes sensibles.

Engagement de Tous les Niveaux Hiérarchiques

- Un effort collectif, impliquant tous les niveaux de l'organisation, du personnel administratif aux cadres dirigeants. Les dirigeants doivent montrer l'exemple en respectant les politiques de sécurité et en encourageant une culture de la protection des données.
- L'engagement des dirigeants est essentiel pour obtenir un soutien organisationnel complet pour les initiatives de sécurité, et pour assurer que les politiques de protection des données sont prises au sérieux à tous les niveaux

05

Responsabilités et Rôles

Responsabilités et Rôles

Les Acteurs Internes

- Responsable de traitement des données : l'entité ou l'individu au sein d'une institution qui détermine les finalités et les moyens du traitement des données personnelles. Rôle souvent assumé par les dirigeants du ministère ou par des responsables désignés. Obligations spécifiques:
  - Réalisation d'analyses d'impact sur la protection des données pour évaluer les risques liés aux activités de traitement.
  - Tenue d'un registre des activités de traitement des données, documentant les types de données traitées, les finalités du traitement, les mesures de protection mises en place, et les partenaires impliqués.

Responsabilités et Rôles

Les Acteurs Internes

- Responsable de la Protection des Données : Responsable de superviser la conformité aux régulations de protection des données au sein de l'institution.
  - Conseiller l'organisation sur ses obligations légales et agir comme point de contact avec l'autorité de protection des données.
  - Sensibiliser le personnel aux obligations en matière de protection des données et de réaliser des audits internes pour s'assurer de la conformité.
  - Doit avoir un accès direct à la direction de l'organisation et disposer des ressources nécessaires pour accomplir ses missions efficacement.
  - Définir les conditions dans lesquelles la nomination d'un DPO est obligatoire, par exemple dans les organisations publiques ou lorsque des traitements de données à grande échelle sont effectués.

Responsabilités et Rôles

Les Acteurs Internes

- Equipe IT et sécurité : Rôle crucial dans la mise en œuvre des politiques de protection des données, en déployant les technologies de sécurité, en surveillant les systèmes, et en réagissant aux incidents de sécurité.
  - Compétences spécifiques requises pour ces équipes: la gestion des systèmes d'information, la cybersécurité, et la cryptographie.
  - Besoin de formation continue pour rester à jour avec les évolutions technologiques et les nouvelles menaces.
  - Besoin de collaboration étroite entre les équipes IT, les équipes de sécurité, et le DPO. Ces équipes doivent travailler ensemble pour identifier les risques, mettre en œuvre des solutions techniques appropriées, et assurer la conformité aux régulations de protection des données..

Responsabilités et Rôles

Collaboration et Coordination

- Collaboration Interservices : Encourager la collaboration entre les différents services au sein de l'institution pour assurer une protection efficace des données. Par exemple, les services juridiques, IT, et RH doivent travailler ensemble pour s'assurer que les politiques de protection des données sont intégrées dans tous les aspects des opérations du ministère.
- Mécanisme de coordination: Définir des mécanismes de coordination tels que des comités de sécurité des données, des réunions régulières entre les différents services concernés, et des processus de révision des politiques de protection des données.

Responsabilités et Rôles

Les Acteurs Externes

- Sous-traitants et Prestataires de Services : qui traitent des données pour le compte de l'institution ont également des responsabilités en matière de protection des données. Cela inclut les entreprises qui fournissent des services cloud, des logiciels, ou des solutions de traitement des données.
  - Ils doivent garantir la sécurité des données qu'ils traitent, respecter les instructions données par le ministère, et notifier immédiatement en cas de violation de données.
  - Inclure des clauses spécifiques de protection des données dans les contrats avec les sous-traitants et les prestataires. Ces clauses doivent préciser les obligations en matière de sécurité, les droits du ministère en cas d'audit, et les procédures de notification en cas d'incident.
  - Ces contrats doivent également prévoir des sanctions en cas de non-respect des obligations de protection des données par le sous-traitant.

Responsabilités et Rôles

Les Acteurs Externes

- Partenaires et Collaborateurs : collaborations avec d'autres ministères, agences gouvernementales ou organisations internationales, le partage des données doit être encadré par des accords de protection des données qui précisent les responsabilités de chaque partie.
  - Définir des mesures à mettre en place pour garantir que les données partagées sont protégées de manière adéquate, y compris des politiques de chiffrement, de restriction d'accès, et de suivi des transferts de données.
  - Chaque partie doit assumer la responsabilité partagée de la protection des données. Cela inclut la mise en place de procédures conjointes pour la gestion des incidents de sécurité et la conformité aux régulations internationales applicables.
  - Transparence et de la communication régulière entre les partenaires pour s'assurer que toutes les parties respectent leurs obligations en matière de protection des données.

06

Conclusion

Conclusion

Importance de la Protection des Données

- Gestion responsable des données est essentielle pour préserver la vie privée des citoyens, maintenir la confiance publique, et assurer la sécurité nationale.
- La protection des données ne concerne pas seulement la conformité légale, mais aussi la prévention des risques et la sécurisation des informations sensibles contre les menaces actuelles et futures.

Synthèse des stratégies

- Politiques et Procédures: Elaboration et mise en œuvre de politiques internes robustes pour la protection des données. Procédures pour la collecte, le traitement, et la conservation des données, ainsi que pour la gestion des incidents de sécurité. Mise à jour régulière de ces politiques pour les aligner sur les évolutions technologiques et les nouvelles régulations
- Technologies de Protection: Utilisation des technologies pour la protection des données, telles que le chiffrement, les pare-feux, et les systèmes de détection d'intrusion. Ces technologies doivent être correctement mises en œuvre et régulièrement mises à jour pour rester efficaces. Elles doivent être soutenue par des politiques et des pratiques solides.

Conclusion

•Rôles et responsabilités

- Les rôles clés des acteurs internes et externes dans la protection des données
  - les responsabilités du délégué à la protection des données
  - les responsables de traitement, et des sous-traitants.
  - Besoin de collaboration et la coordination entre ces acteurs pour une gestion efficace des données.
- Formation continue et sensibilisation pour s'assurer que tous les employés comprennent leurs responsabilités en matière de protection des données.

Évolution des Menaces

- Menaces à la sécurité des données évoluent constamment, en raison des progrès technologiques et de l'ingéniosité des cybercriminels. Les institutions doivent adopter une approche dynamique et proactive, en intégrant les dernières technologies et en s'adaptant aux nouvelles régulations.
- Responsabilité Collective: la protection des données est une responsabilité collective qui implique tous les membres de l'organisation, des dirigeants aux employés.

Dans notre institution

1. Avons-nous un plan de gouvernance des données?
2. Quelles sont les difficultés à mettre sur pied un plan de gouvernance des données?
3. Avons-nous des stratégies en interne pour la protection des données ?
4. Les rôles et responsabilités sont-ils définis?
5. Avons-nous des mécanismes d’évaluation?
6. Les stratégies sont-elles efficaces?
7. Avez-vous des pistes d’amélioration?

MERCI!

QUESTIONS?

lfendji@gmail.com
+237 677038781/ 655811916