Titre du projet	Collectez des données en respectant les normes RGPD

Version	Auteur	Description	Date
V1	*MOHAMED YEHDIH Neyna*	Rapport de traitement des données	*14.08.2024*

Introduction

Dev'Immediat, courtier en assurance automobile, traverse une période critique après avoir été sanctionnée par la CNIL pour non-respect du RGPD.

Cette sanction a plongé l'équipe dans un climat de stress et d'incertitude, car la continuité des activités commerciales de l'entreprise dépend de la résolution rapide de ce problème.

Les collaborateurs ressentent une pression intense, avec un besoin urgent de solutions efficaces pour se conformer aux exigences légales.

Dev'Immediat doit impérativement réviser ses processus de collecte et de traitement des données pour garantir leur conformité avec le RGPD, tout en assurant la protection des données personnelles de ses clients. Cette révision est d'autant plus cruciale que l'entreprise doit continuer à exploiter les données nécessaires à ses activités, malgré les restrictions temporaires imposées.

L'objectif principal de **Dev'Immediat** est de retrouver une pleine conformité avec le RGPD, afin de lever les sanctions et de garantir la pérennité de l'entreprise. En parallèle, elle doit maintenir la continuité de ses activités commerciales, notamment la prospection et la vente de contrats d'assurance, qui sont essentielles pour son modèle économique.

Les enjeux sont multiples : sur le plan légal, il s'agit de respecter strictement les obligations du RGPD pour éviter des sanctions plus sévères ; sur le plan commercial, de maintenir la capacité à traiter les données nécessaires pour piloter la performance ; et sur le plan réputationnel, de restaurer la confiance des clients et des partenaires.

Si **Dev'Immediat** parvient à surmonter cette situation, elle bénéficiera d'une conformité juridique renforcée, d'une continuité des activités avec un impact minimal, et d'une amélioration de sa réputation, en démontrant son engagement envers la protection des données de ses clients.

Contenu du rapport :

I. Préconisations en Lien avec les Règles RGPD

Pour garantir à l'avenir le respect du RGPD et éviter de nouvelles sanctions, **Dev'Immediat** doit mettre en place des mesures strictes conformes aux principes du RGPD, notamment des préconisations spécifiques concernant la collecte et le traitement des données, avec un accent particulier sur la transparence, les droits des personnes, et la sécurisation des données.

1. Collecte des Données

a) Transparence et Information des Clients

- **Politique de Confidentialité** : Rédiger une politique de confidentialité claire et accessible, expliquant comment les données des clients sont collectées, utilisées, stockées, et partagées.
- **Communication d'Information** : Informer les clients dès la collecte des données sur leurs droits et l'usage qui sera fait de leurs informations, cela inclut :
  - La finalité du traitement des données.
  - La base légale du traitement (par exemple, consentement, obligation légale).
  - Les destinataires des données.
  - La durée de conservation des données.
  - Le droit de retirer leur consentement à tout moment.

b) Consentement Explicite

- **Obtention du Consentement** : Assurer que le consentement est libre, spécifique, éclairé, et univoque pour chaque traitement.

  Utiliser des cases à cocher non pré-cochées et un langage compréhensible.
- **Gestion du Consentement** : Mettre en place des outils permettant aux clients de gérer leurs préférences et de retirer leur consentement facilement.

c) Minimisation des Données

- **Collecte Nécessaire** : Ne collecter que les données strictement nécessaires aux finalités spécifiques pour lesquelles elles sont recueillies. Éviter la collecte de données sensibles sauf en cas de nécessité et avec des mesures de protection renforcées.
- **Révision des Données Collectées** : Évaluer régulièrement les types de données collectées pour s'assurer qu'elles restent pertinentes et minimales.

2. Traitement des Données

a) Sécurisation des Données

- **Mesures de Sécurité Techniques** : Implémenter des mesures de sécurité adéquates pour protéger les données personnelles contre les accès non autorisés, les pertes, ou les fuites. Cela inclut le chiffrement, l'anonymisation, et la pseudonymisation des données lorsque c'est possible.
- **Contrôle d'Accès** : Limiter l'accès aux données personnelles aux seules personnes ayant besoin d'y accéder dans le cadre de leurs fonctions.

b) Conservation et Suppression des Données

- **Politique de Conservation** : Mettre en place une politique de conservation des données, définissant clairement les périodes de conservation en fonction des finalités et des obligations légales. Après expiration de la période de conservation, les données doivent être supprimées ou anonymisées de manière irréversible.
- **Suivi de la Suppression** : Utiliser des outils pour automatiser la suppression des données après la fin de la période de conservation ou en cas de retrait du consentement par le client.

c) Gestion des Droits des Personnes

- **Accès et Rectification** : Permettre aux clients d'accéder à leurs données et de les rectifier facilement. Une interface utilisateur dédiée peut faciliter ces opérations.
- **Portabilité des Données** : Fournir aux clients la possibilité de récupérer leurs données dans un format structuré, couramment utilisé, et lisible par machine.
- **Droit à l'Oubli** : Mettre en place des procédures efficaces pour répondre aux demandes de suppression des données des clients, conformément au droit à l'oubli.
- **Opposition et Limitation du Traitement** : Respecter les demandes des clients souhaitant limiter le traitement de leurs données ou s'y opposer, en particulier pour les traitements à des fins de prospection commerciale.

3. Gouvernance et Sensibilisation

a) Délégué à la Protection des Données (DPO)

- **Nomination d'un DPO** : Désigner un Délégué à la Protection des Données (DPO) chargé de superviser la conformité RGPD, de former le personnel, et de servir de point de contact avec la CNIL et les clients.

b) Formation Continue

- **Formation des Équipes** : Former régulièrement les équipes sur les exigences du RGPD et les bonnes pratiques en matière de protection des données personnelles.
- **Sensibilisation à la Sécurité** : Organiser des sessions de sensibilisation à la cybersécurité pour tous les employés, en mettant l'accent sur la protection des données et la détection des menaces potentielles.

II. Mesures à Prendre Par Dev'Immediat

A. Analyse et Correction des Processus de Collecte et de Traitement des Données

Dev'Immediat doit immédiatement procéder à un audit complet des processus de collecte et de traitement des données pour identifier les pratiques non conformes au RGPD.

Les points suivants doivent être vérifiés et, si nécessaire, corrigés :

1. **Consentement explicite des clients** : Assurez-vous que les données collectées sont accompagnées d'un consentement clair et spécifique de chaque client.
2. **Minimisation des données** : Ne collectez et ne conservez que les données strictement nécessaires aux finalités déclarées. Évitez de collecter des données personnelles extensives ou non pertinentes comme le groupe sanguin, nom, le Num_ss ...etc.
3. **La transparence :** Les individus doivent être informés de manière claire et compréhensible sur le traitement de leurs données personnelles. Mettez en place une politique de confidentialité claire et accessible, expliquant comment les données personnelles sont collectées, utilisées, protégées et les droits des individus.
4. **Conservation des données** : Mettez en place une politique de conservation des données qui respecte les délais légaux et évitez la conservation indéfinie des informations personnelles.
5. **Obligation de sécurité :** Les données sensibles, comme les groupes sanguins, doivent être protégées par des mesures spécifiques, incluant le chiffrement des données, la pseudonymisation et l'anonymisation pour protéger les données personnelles contre les accès non autorisés, les pertes, ou les fuites et minimiser les risques d'identification.

B. Collaboration avec la CNIL

Engagez un dialogue avec la CNIL pour démontrer la volonté de **Dev'Immediat** de se conformer aux régulations. Présentez un plan d'action détaillé pour corriger les infractions et demandez des clarifications sur les attentes de l'autorité régulatrice.

C. Mise en Place de Mesures Transitoires

Pendant la période de limitation, **Dev'Immediat** peut envisager les actions suivantes pour limiter l'impact sur ses opérations :

- **Anonymisation des Données** : Explorez la possibilité d'anonymiser les données pour les traiter sans enfreindre la limitation. Ceci pourrait permettre la poursuite des analyses de performances sans compromettre la confidentialité des clients.
- **Utilisation de Données Agrégées** : Utilisez des données agrégées ou statistiques qui ne permettent pas l'identification des individus pour continuer à piloter la performance commerciale.
- **Renforcement des Formations** : Formez les équipes sur les bonnes pratiques de gestion des données personnelles pour éviter de futures violations.

III. Documentation des traitements effectués

La documentation des traitements effectués est cruciale pour assurer la traçabilité, la transparence, et la conformité aux exigences légales et réglementaires. Cela inclut :

a. Documentation de la requête SQL utilisée pour extraire les données

```
38 SELECT id_client, date_naissance, sexe, nombre_enfants,
39 revenus, formule, tarif_devis, date_demande,
40 enfant_conduite_accompagne, usage_vehicule, age_vehicule,
41 type_vehicule, points_perdus, type_conduite
42 FROM base_client
43 WHERE strftime('%Y', date_demande)  = "2022" AND etat_dossier = "complet
44 ;
```

Cette requête permet l'extraction des **variables** strictement nécessaires à mettre à disposition de l'équipe de performance commerciale de **Dev'Immediat** pour qu'elle puisse continuer à travailler, ainsi que les données de la demande d'assurance effectuées en **2022** pour les clients dont l'état dossier est « **complet** » à partir de la base **SQL.**

b. Documentation des étapes de traitement du fichier Power Query

Les étapes de traitement effectuée dans Power Query pour nettoyer les données :

Importation des données :

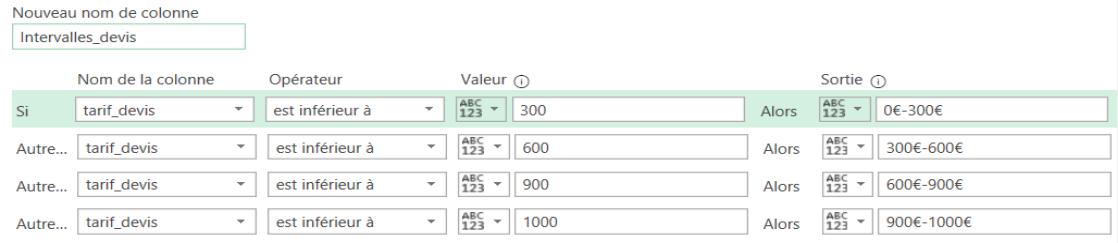
- Chargement des données brutes depuis la base de données.

Filtrage :

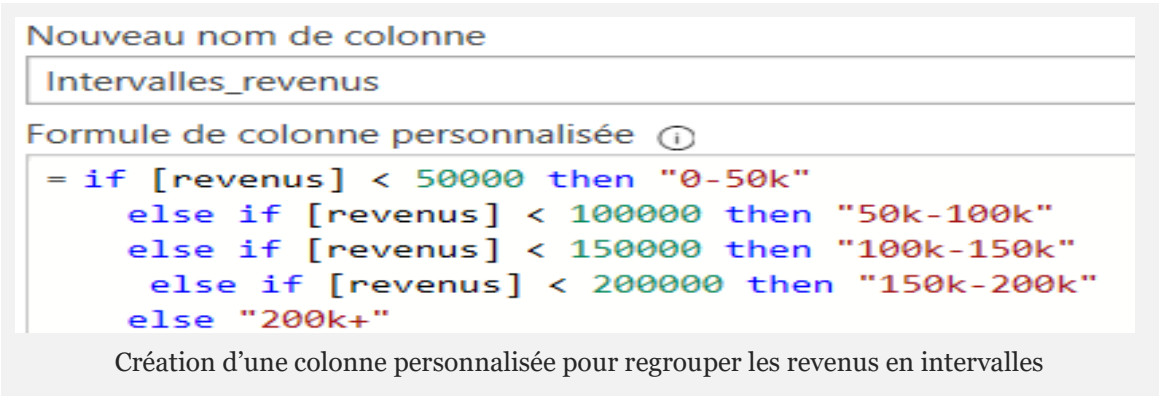
- Suppression des colonnes inutiles
- Remplacement des valeurs
- Extraction des caractéres
- Correction des types de données…etc

Transformation :

- Création d'une colonne personnalisée pour regrouper les revenus en intervalles.
- Création d'une colonne personnalisée pour regrouper les tarif_devis en intervalles.
- Création d'une colonne personnalisée présence d'enfant par une valeurs binaire.



Création d'une colonne personnalisée pour regrouper les tarif_devis en intervalles



Création d'une colonne personnalisée pour regrouper les revenus en intervalles

Anonymisation :

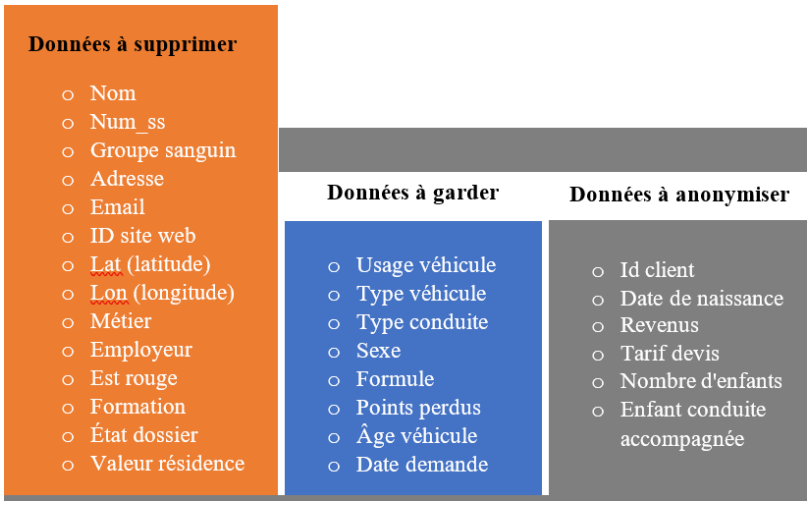
- Remplacement de l'identifiant client par un index personnalisé.
- Remplacement de la colonne date_naissance par une colonne age.

Création d'une colonne personnalisée présence d'enfant par une valeur binaire

c) Documentation des traitements effectués sur la base de données brutes

Les transformations appliquées directement sur les données brutes avant leur intégration dans les systèmes de traitement:

- ☞ Préparation des données pour le nettoyage : suppression des données à carectére personneles, sensibles ou inutiles pour l'analyse.
- ☞ Vérification de l'intégrité des données : les doublons, aucune ligne ne doit avoir de valeurs nulles dans les colonnes obligatoires.



d) Etapes pour retravailler le jeu de données et les explications associées

Agrégation :

- ☞ Regrouper les données par catégorie (par exemple la demande d'assurance effectuée en 2022) pour des analyses statistiques.

Filtrage avancé :

- ☞ Application de critères supplémentaires pour exclure des sous-ensembles spécifiques (ex : clients ayant des dossiers incomplets).

Conclusion

La situation actuelle oblige **Dev'Immediat** à réévaluer ses pratiques de gestion des données. En mettant en place rapidement des mesures correctives et en coopérant pleinement avec la CNIL, l'entreprise peut non seulement surmonter cette crise, mais aussi renforcer ses processus de conformité pour l'avenir.

Ces recommandations permettront à **Dev'Immediat** de se conformer aux exigences actuelles de la CNIL tout en solidifiant durablement ses pratiques en matière de gestion des données. En adoptant une approche proactive et rigoureuse, l'entreprise pourra non seulement éviter de nouvelles sanctions, mais aussi établir une relation de confiance avec ses clients, fondée sur la transparence et le respect de leur vie privée.

Dans un contexte où la protection des données personnelles est devenue un enjeu majeur, notamment avec le RGPD, il est crucial pour des entreprises comme **Dev'Immediat** de s'adapter aux exigences croissantes en matière de confidentialité. Cette adaptation ne se limite pas à la conformité légale, mais inclut également la mise en place de pratiques éthiques qui renforcent la confiance des clients et assurent la pérennité des activités commerciales.

Exigences : Les entreprises doivent mettre en place des processus robustes pour garantir la transparence dans la collecte et le traitement des données, tout en respectant les droits des individus (accès, rectification, suppression des données, etc.). Ces exigences impliquent une documentation rigoureuse, des audits réguliers, et une sensibilisation continue des équipes aux enjeux de la confidentialité.

Contraintes : La mise en conformité avec le RGPD peut parfois imposer des contraintes significatives, notamment en termes de ressources humaines, financières, et technologiques. Les entreprises doivent jongler avec ces contraintes tout en maintenant une efficacité opérationnelle. De plus, l'évolution rapide des réglementations exige une veille constante et une capacité à adapter rapidement les processus internes.

Enjeux : La confidentialité des données n'est pas seulement une obligation légale, mais un facteur clé de la relation de confiance entre une entreprise et ses clients. En cas de non-conformité, les entreprises risquent non seulement des sanctions financières et légales, mais aussi une dégradation de leur réputation. En revanche, une gestion exemplaire des données personnelles peut constituer un avantage concurrentiel, en renforçant la fidélité des clients et en attirant de nouveaux partenariats.

Face à ces exigences, contraintes et enjeux, il est essentiel pour **Dev'Immediat** de continuer à investir dans des solutions techniques, organisationnelles, et humaines pour assurer la confidentialité des données, tout en maintenant une performance commerciale optimale. L'avenir des entreprises dépendra en grande partie de leur capacité à naviguer dans cet environnement complexe et exigeant, où la confidentialité des données est devenue un pilier fondamental de la réussite.