Compte-rendu GT Normalisation #5

04 Février 2021

Chantier SMILE, Projet SEN, Groupe de travail « Normalisation Quoalise »

Tableau de suivi des versions

Version	1			
Auteurs	EM			
Date	11/03/21			
Commentaires	Version initiale			

TABLE DES MATIÈRES

Participants....3
Questions Juridiques....3
1 Recueil du consentement....3
Quels canaux « numérisables » peuvent être juridiquement utilisés pour recueillir un consentement ?....3
Jusqu'où doit aller la non-répudiabilité vis à vis de l'appréciation d'un juge sur la qualité des preuves ?....4
2 Responsables de Traitement en fédération....6
Le consentement au traitement peut-il couvrir le transfert de données via la fédération ? 6
Y a t'il besoin de contractualisation (co-traitance, sous-traitance) entre instances (personne morale ou physique qui fait tourner un logiciel connecté à la fédération et qui procède à des transferts de données personnelles) de la fédération ?....6
3 Liens contractuels au sein de la fédération....6
Quels sont les liens contractuels nécessaires et possibles entre nœuds de la fédération (ou entre un nœud et une entité utilisatrice de ce nœud) : co-traitance, sous-traitance, ... ?....6
Recommandations SEN pour le RGPD....7

PARTICIPANTS

- Elias Martin, consometers et projet Quoalise
- Cyril Lugan, consometers et projet Quoalise
- Gautier Husson, consometers et projet Quoalise
- Lydie LE FLOCH, GRDF : mise à dispo offres de données à l'externe, contrôle de consentement (addict), accompagnement des projets territoriaux sur 3 région
- Charlotte BOSCH, Enedis : juriste spécialiste des sujets data
- Chloé VENEZIA, Enedis : juriste de la mission Informatique et Libertés
- Fabien COUTANT, Enedis : Direction du Numérique, gouvernance des données, API dont data connect
- Nicolas VIEL : Enedis, Direction Bretagne

QUESTIONS JURIDIQUES

NB : il s'agit de réponses adaptées au contexte Enedis et GRDF propre, qui peuvent ne pas être adaptées à des contextes différents et qui ne valent pas conseil juridique. Ce sont les exemples de leur côté.

1 Recueil du consentement

Quels canaux « numérisables » peuvent être juridiquement utilisés pour recueillir un consentement ?

* Enedis : la règlementation n'impose pas de canal particulier, elle impose surtout que toutes les infos nécessaires à un consentement soient présentes, et que l'on peut en apporter la preuve. Le consentement doit notamment être libre, éclairé, spécifique, univoque.

* Enedis : la CNIL a récemment lancé une consultation sur l'exercice des droits par les personnes via un acteur mandaté qui peut également fournir des éléments : https://www.cnil.fr/fr/consultation-publique-projet-recommandation-mandat

* Enedis : la CNIL nous laisse des largeurs (pas de restriction de moyen technique) => Mais il faut en apporter la preuve et recueillir le consentement selon les critères fixés.

* Enedis : il faut également s'assurer sur les canaux numériques que la personne qui donne son consentement est bien celle qu'elle prétend être et qu'elle habite bien à l'adresse indiquée. Par

exemple pour identifier le client sur le portail Enedis, nous proposons 3 manière de s'identifier : par un courrier reçu à domcilie, par FranceConnect et comparaison du nom retourné avec celui du titulaire du contrat de fourniture d'électricité, ou bien en fournissant des informations présentes sur la carte d'identité et la facture d'électricité et en comparant le nom de la carte d'identité avec celui du titulaire du contrat de fourniture d'électricité.

* Enedis : les tiers peuvent aussi être chargé de collecter le consentement. Pour les preuves sur canaux numériques, nous demandons aux acteurs de nous fournir des traces de connexion et IP (méthode mise en oeuvre chez Enedis, sans obligation spécifique juridique). L'appréciation du risque est laissée à chacun

Jusqu'où doit aller la non-répudiabilité vis à vis de l'appréciation d'un juge sur la qualité des preuves ?

* Un log / une trace de bdd est altérable

* le responsable de traitement doit être en mesure de prouver qu'il a bien recueilli le consentement

* en pratique on peut remettre en cause plein de chose

* pour Enedis, le risque zéro n'existe pas, mais nous pouvons (dans le cas où la preuve est répudiable) nous reposer sur un faisceau d'indices accumulés qui conduisent à une preuve viable

* Enedis : à noter qu'il y a peu de jurisprudences à ce jour sur la répudiabilité de la preuve. Il y a plutôt des décisions de la CNIL sur les étapes amont (modalités d'obtention du consentement, clarté du process, conservation des données etc...), pas sur la technique elle-même). Un point essentiel du consentement est l'information des personnes (consentement spécifique, univoque, éclairé)

* Avis / expériences sur les procédés de signature numérique, non répudiabilité

* Méthodes d'identification (préalable au consentement) :

* GRDF Adict "Client Connect" en lancement : via adresse mail par exemple (pour autorisation du transfert de données) mais également compte GRDF en ligne (identifié par code PCE et code postal)

* Autre appréciation du risque et des données : Données peut êtres moins sensibles

* Enedis

* Carte d'identité + facture

* France Connect

* Courrier

* Lite

* Upload de factures

* Enedis : identification = préalable du recueil de consentement, "filtre", car on sait que ce sont les données concernant la personne

* on peut avoir de tout (ex : upload de facture, ou rien ...)

* ? quelle obligation ? la CNIL apprécie en fonction des efforts mis dans le processus et dans la tentative d'usurpation.

* Usage de France Connect ? Quelles sont les limites d'accès par un fournisseur de services ?

* https://franceconnect.gouv.fr/partenaires

* conditions pour les privés : https://franceconnect.gouv.fr/partenaires#can-you-integrate-fc-entreprise

* Comment gérer la délégation d'action auprès de conseillers info-énergie ?

* Exemple en ALEC auprès de public en précarité énergétique (logements sociaux...)

* GRDF :

* Ex mail GRDF

* Consentement données

* + Je mantate tel tiers pour recevoir le mail de vérification / création de compte

* .En cas d'impossibilité de la part du Titulaire de valider cet email (ex : non accès à internet), le Tiers peut recueillir un mandat du Titulaire pour le transfert des données et pour la prise en charge de l'email de validation. Cette mention doit alors clairement apparaitre dans le mandat.

* cadre d'une collectivité : le syndicat d'énergie donne son consentement ou est mandaté

* Enedis : si le responsable de traitement mandate une autre société pour récupérer le consentement d'une personne, le consentement collecté par la société doit aussi mentionner le responsable de traitement initial. Attention du coup au caractère éclairé du consentement ! Et entre les deux entités, on suggère que les "clauses RGPD" soient bien dans le contrat (voir modèle de la CNIL https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses)

2 Responsables de Traitement en fédération

Le consentement au traitement peut-il couvrir le transfert de données via la fédération ?

Y a t'il besoin de contractualisation (co-traitance, sous-traitance) entre instances (personne morale ou physique qui fait tourner un logiciel connecté à la fédération et qui procède à des transferts de données personnelles) de la fédération ?

* Enedis : ce qui semble a priori logique vu ce qui a été présenté est un modèle de sous-traitance (la société le plus loin est responsable de traitement et les coeuds intermédiaires sont sous-traitants). la co-traitance paraît plus compliquée car le consentement sera porté par toute la chaine et devra être explicite.

* Enedis : même dans une logique communautaire très ouverte, des sortes de CGU de prestation de service d'un noeud à un autre pourraient mieux définir le qui fait quoi tout en restant souple et accueillir facilement de nouveaux noeuds.

* La transmission des données est un traitement de données ?

* Enedis : oui, et ce quel que soit le volume de données transféré ou la durée pendant laquelle est est stockée ou mise en tampon etc.

* analogie au mail : pas sécurisé en terme fonctionnel, technique => situation possible (dans une certaine mesure) mais risques importants en complexité. En restant sur du communautaire, il faut réflechir à des CGU qui explicitent la situation.

3 Liens contractuels au sein de la fédération

Quels sont les liens contractuels nécessaires et possibles entre nœuds de la fédération (ou entre un nœud et une entité utilisatrice de ce nœud) : co-traitance, sous-traitance, ... ?

* Enedis : => SLA, responsabilités entre entités, résolution de problèmes => nous semble important de contractualiser

* Est ce que la transmission d'informations est un traitement au sens du RGPD ? cf Directive eCommerce et "mere conduit"

* https://en.wikipedia.org/wiki/Electronic_Commerce_Directive_2000#Mere_conduit

* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32000L0031

* => oui pour Enedis et GRDF

Recommandations SEN pour le RGPD

Dans notre étude du RGPD, nous avions émis ces recommandation, vous paraissent elles pertinentes ? Dans le cadre de la fédération, le recueil du consentement peut s'envisager selon deux modalités :

1. Le consentement est laissé à la charge de l'application « initiale » qui en transfère une preuve à l'application « secondaire », et assume l'ensemble de la responsabilité de traitement. Et dans ce cas, deux possibilités :

Cas 1) la contractualisation entre les deux entités juridiques (sous-traitance).

Cas 2) l'entité responsable de l'application initiale recueille les traitements opérés par l'application secondaire et fait directement consentir l'utilisateur aux deux traitements. A noter, le chaînage peut se faire avec un nombre indéterminé d'applications et d'entités juridiques.

2. La demande de consentement est transmise à l'application « secondaire » qui le recueille selon ses propres modalités, puis transmet les données concernées à l'application « initiale ».

Pour Enedis : la définition fine du mode d'accès et des API les rend responsable pour la '"Transmission de données". En revanche le Tiers est responsable de tous les autres usages des données.