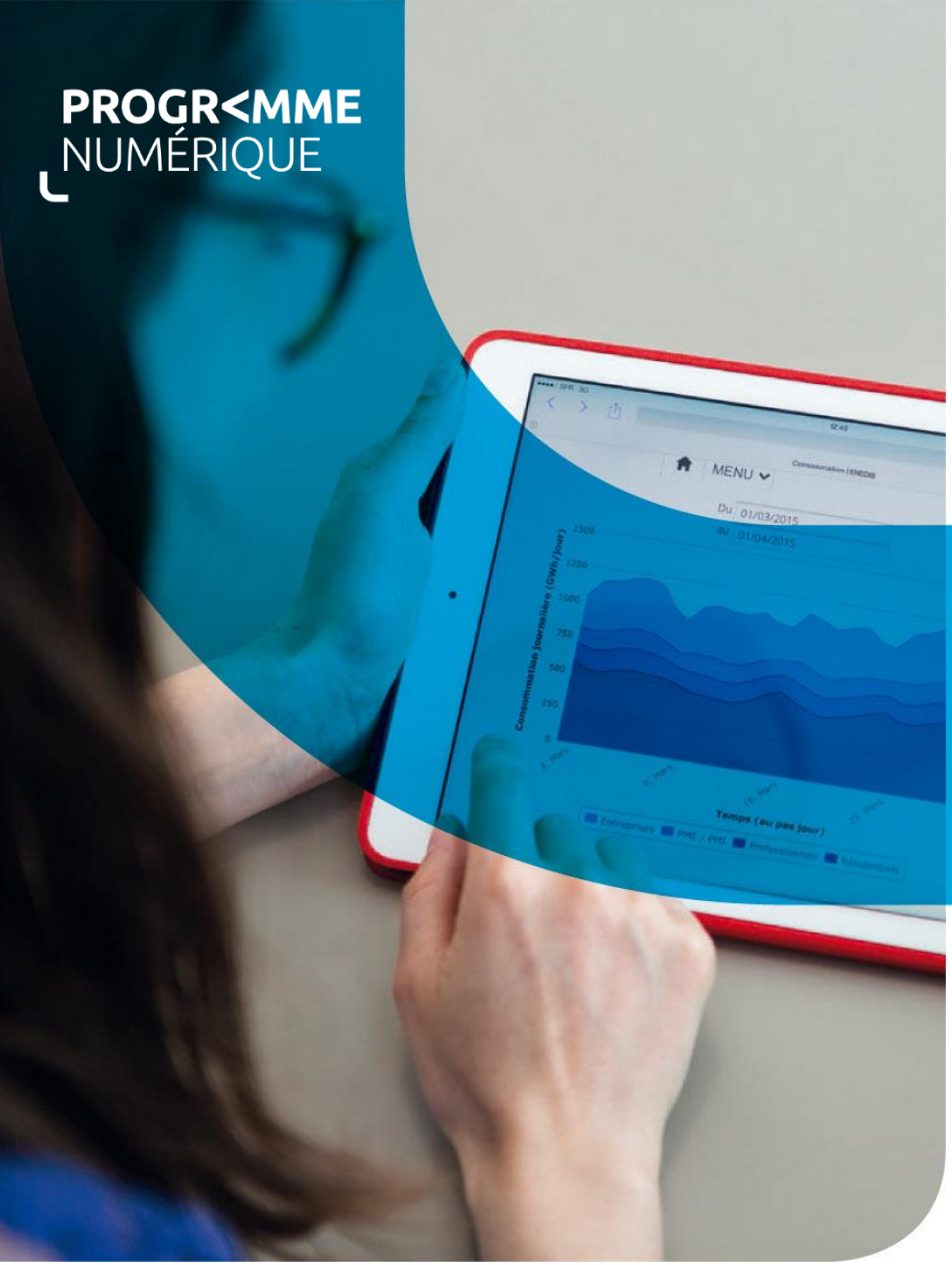
PROGR<MME
NUMÉRIQUE



RGPD et protection de données

Mars 2018

ENEDIS
L'ELECTRICITE EN RESEAU

Les types d'information qui doivent être protégés par les acteurs qui manipulent les données

DCP

Donnée à Caractère Personnel
Données permettant d'identifier, directement ou indirectement, une personne physique

ICS

Information Commercialement Sensible
Information dont la communication serait dommageable à une concurrence libre et loyale

DSP

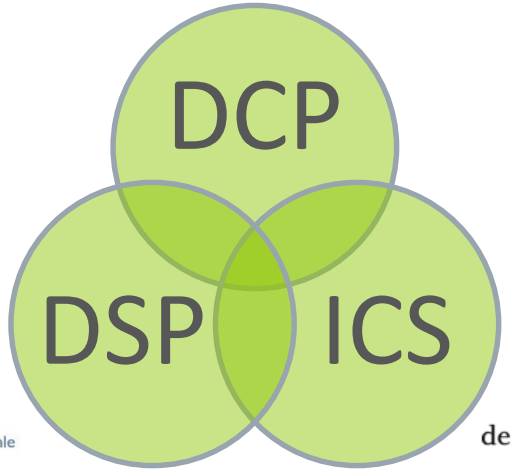
Donnée sensible eu égard à la Sécurité Publique
Informations confidentielles eu égard aux impératifs de sécurité publique

Indus.

Donnée à protéger au titre du secret industriel et commercial
Informations à protéger au titre du secret des procédés, des informations économiques et financières et des stratégies commerciales

De la nécessité de protéger les données
Et de créer les conditions de la confiance

CNIL
Commission Nationale de l'Informatique et des Libertés



ANSSI
Agence nationale de la sécurité des systèmes d'information

Autorité de la concurrence

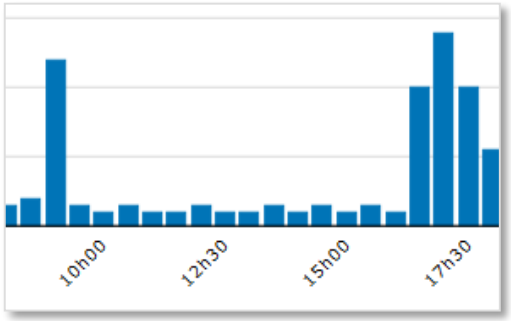
COMMISSION DE RÉGULATION DE L'ÉNERGIE

Données à caractère personnelle (règlement européen et loi 78-17)

Informations commercialement sensibles (droit de la concurrence et art. L. 111-72, L. 111-73 et L. 111-77 du code de l'énergie)

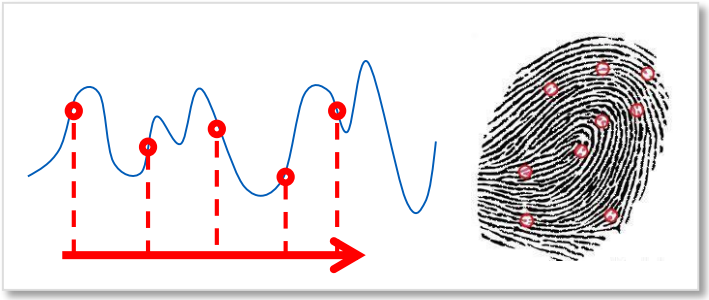
Opérateur d'infrastructure d'importance vitale (art. R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense)

Nécessité de protéger la confidentialité des données énergétiques



Les données de consommation sont révélatrices de comportement individuels ou de groupe qui peuvent porter atteinte à la vie privée des clients et aux secrets des entreprises

Elles constituent une véritable empreinte des clients : une suite de plusieurs niveaux de consommation d'un client est unique parmi 300 000 clients.



Une fois croisées ou retravaillées avec d'autres tiers, elles peuvent permettent d'inférer des comportements. À New York, un Open Data réputé anonyme à partir des données de mobilité des taxis a permis par croisement de reconstituer des usages individuels et groupés

Démarche RGPD en cours de mise en place au sein d'Enedis

Pour rappel : Applicable à partir du 25 mai 2018 à l'ensemble de l'Union européene, le Réglementation européen sur la Protection des Données (RGPD) renforce les droits des résidents européens sur leurs données et responsabilise l'ensemble des acteurs traitant ces données (Responsable de Traitement et Sous-Traitants) qu'ils soient établis ou non au sein de l'Union Européenne.

* démarche préconisée par la CNIL : rgpd-se-preparer-en-6-etapes

Démarche RPDG en cours de mise en place au sein d'Enedis

ETAPE 4 GÉRER LES RISQUES	**GÉRER LES RISQUES** Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA).
ETAPE 5 ORGANISER	**ORGANISER LES PROCESSUS INTERNES** Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).
ETAPE 6 DOCUMENTER	**DOCUMENTER LA CONFORMITÉ** Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

* démarche préconisée par la CNIL : rgpd-se-preparer-en-6-etapes

En conclusion

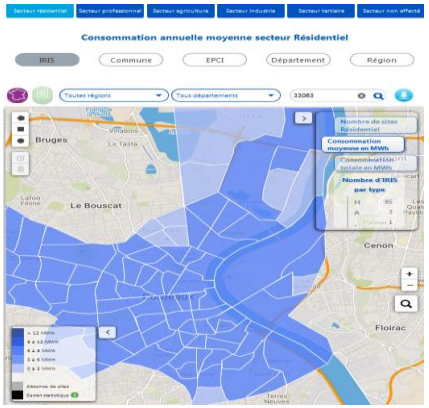
La protection des données de ses clients est une priorité d'Enedis.

Les données de consommation des clients ne peuvent être **transmises qu'avec leur consentement libre, éclairé et spécifique**. A défaut, elles doivent être **agrégées à une maille permettant de garantir la protection** des Données à Caractère Personnel, du Secret des Affaires et des Informations Commercialement Sensibles, **ou être anonymisées**.

Données à accès restreint : Enedis transmet aux Collectivités et aux acteurs publics, au titre de leurs compétences, certaines données à un niveau d'agrégation plus fin, secrétisées ou non. Ces données sont à accès restreint (*closed data*). Les Collectivités portent la responsabilité de protéger les données sensibles transmises par Enedis.

Open data: des données anonymisées ou agrégées, ouvertes à tous, gratuitement.

http://www.enedis.fr/open-data



MERCI POUR VOTRE ATTENTION

Retrouvez-nous sur Internet

enedis.fr

enedis.officiel

@enedis

enedis.officiel