Recommandation de la branche

Politique des données dans la branche énergétique

Cadre de gestion globale des données dans la branche énergétique

DPE – CH 2022

Impressum et contact

Éditeur
Association des entreprises électriques suisses AES
Hintere Bahnhofstrasse 10
CH-5000 Aarau
Téléphone +41 62 825 25 25
Fax +41 62 825 25 26
info@electricite.ch
www.electricite.ch

Auteurs de la première édition

"Prénom Nom"	Entreprise	Fonction
Daniel Füglistaller	Axpo	Membre du groupe de travail
Gunnar Greiter	Sysdex	Membre du groupe de travail
Patrick Hauser	AEW	Membre du groupe de travail
Stéphane Henry	Romande Energie	Responsable du groupe de travail
Christoph Jörg	BKW Energie SA	Membre du groupe de travail
Wolfgang Korosec	Services industriels de Saint-Gall	Membre du groupe de travail
Claudio Maag	EKZ	Membre du groupe de travail
Georg Meier	Axpo	Membre du groupe de travail
Susanne Weidmann	VSE / AES	Secrétariat technique
Jörg Weyermann	esolva	Membre du groupe de travail

Auteurs de la deuxième édition

Daniel Füglistaller	Axpo	Membre de la Task Force
Barbara Gassmann	SIG	Membre de la Task Force
Gunnar Greiter	Sysdex	Membre de la Task Force
Bjoern Gross	IWB	Membre de la Task Force
Patrick Hauser	AEW	Membre de la Task Force
Christoph Jörg	BKW Energie SA	Responsable de la Task Force
Wolfgang Korosec	Services industriels de Saint-Gall	Membre de la Task Force
Claudio Maag	EKZ	Membre de la Task Force
Adrian Mettler	Repower	Membre de la Task Force
Markus Riner	VSE / AES	Secrétariat technique
Vincent Rits	Primeo Netz AG	Membre de la Task Force
Peter Schneider	Energie 360	Membre de la Task Force
Hansjürg Stiffler	Swissgrid	Membre de la Task Force
Jörg Weyermann	esolva	Membre de la Task Force

Responsabilité du groupe de travail
La Task Force Data Policy & Analytics de l'AES est désignée responsable de la tenue à jour et de l'actualisation du document.

Chronologie

Juin 2018	Planification des travaux pour la recommandation de la branche
Juillet 2019	Approbation de la première édition par le Comité de l'AES
Mars 2022	Approbation de la deuxième édition par le Comité de l'AES

Ce document a été élaboré avec l'implication et le soutien de l'AES et de représentants de la branche.

L'AES a approuvé ce document à la date du 23.03.2022.

Imprimé Nº 2002/f, édition 2022

Égalité linguistique des sexes
Pour des raisons de lisibilité, ce document renonce à faire la distinction entre les formes linguistiques masculin, féminin et divers (m/f/d). Toutes les désignations de personnes valent de la même façon pour tous les sexes.

Table des matières

Liste des figures

Liste des tableaux

Avant-propos

Le présent document est un document de la branche publié par l'AES. Il fait partie d'une large réglementation relative à l'approvisionnement en électricité sur le marché de l'électricité. Les documents de la branche contiennent des directives et des recommandations reconnues à l'échelle de la branche concernant l'exploitation des marchés de l'électricité et l'organisation du négoce de l'énergie, répondant ainsi à la prescription donnée aux entreprises d'approvisionnement en électricité (EAE) par la Loi sur l'approvisionnement en électricité (LApEl) et par l'Ordonnance sur l'approvisionnement en électricité (OApEl).

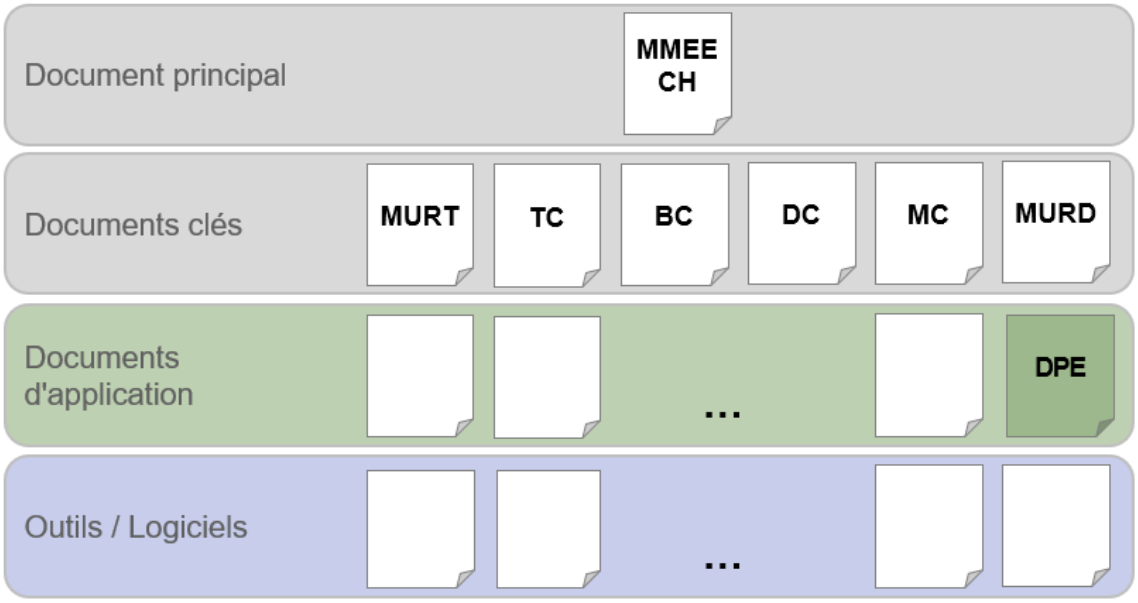
Les documents de la branche sont élaborés par des spécialistes de la branche selon le principe de subsidiarité; ils sont régulièrement mis à jour et complétés. Les dispositions qui ont valeur de directives au sens de l'OApEl sont des normes d'autorégulation.

Les documents sont répartis en quatre catégories hiérarchisées:

- Document principal: Modèle de marché pour l'énergie électrique – Suisse (MMEE – CH)
- Documents clés
- Documents d'application
- Outils/logiciels

Le présent document «Politique des données dans la branche énergétique» constitue un document d'application.

Structure des documents



1. Introduction

1.1 Généralités

(1) Motivée par les besoins des clients et les nouvelles possibilités techniques, la digitalisation confère une importance croissante au traitement et à l'utilisation des données commerciales[1], deux processus générateurs de valeur ajoutée. Les innovations techniques, les vastes bases de données ainsi que les opportunités considérables offertes par l'analyse et la mise en relation des données constituent les fondements d'évolutions inédites de certains secteurs commerciaux, également transposables à la branche énergétique.

(2) Le présent document se fonde sur la Loi fédérale sur la protection des données (LPD) qui entrera probablement en vigueur au 1er janvier 2023. Le 1er janvier 2018, le droit relatif à l'approvisionnement en électricité a fixé les conditions-cadre pour les EAE – en premier lieu dans leur fonction de gestionnaire de réseau – en matière de collecte et de traitement des données des systèmes de mesure, de commande et de réglage intelligents (en particulier art. 17c LApEl, art. 8d OApEl).

(3) Les directives de **séparation au niveau de l'information**, conformément à l'art. 10, al. 2, LApEl, doivent également être prises en compte.

(4) Les infractions aux exigences régulatoires en vigueur en matière de gestion des données **à tous les niveaux de l'organisation,** peuvent donner lieu à des sanctions aussi bien **individuelles** que spécifiques à l'entreprise.

(5) Dans le présent document, le terme d'«utilisateur du réseau» désigne le consommateur final et/ou le producteur et/ou l'exploitant du dispositif de stockage.

1.2 Objectif du document

(1) Le présent document sert de recommandation pour une gestion des données à l'échelle de la branche, régulière et juridiquement conforme, et de politique des données pratique (aussi appelée «Data Policy») pour la branche énergétique. Celle-ci regroupe les principes relatifs aux problématiques pertinentes en matière d'utilisation, de conformité (protection et sécurité) et de gouvernance des données. Ces derniers sont représentés sous la forme de recommandations d'action, de supports et de propositions organisationnelles pour les thèmes stratégiques en matière de données au sein d'une entreprise liée à la branche énergétique.

[1] Y compris les données issues d'activités commerciales

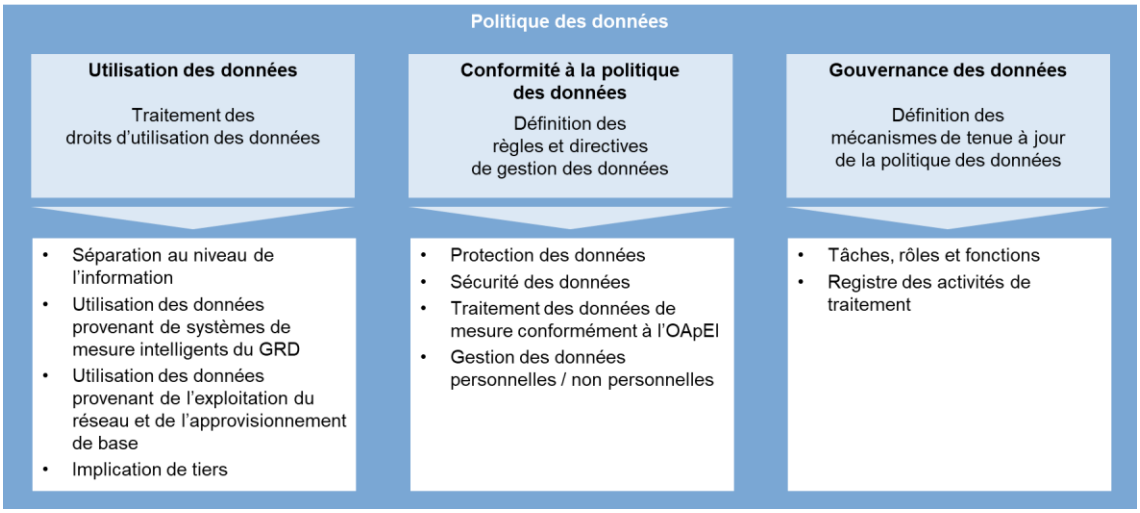


Figure 1 Thèmes-clés de la politique des données

(2) La présente politique des données sert de guide pratique ou d'outil pour les entreprises liées à la branche énergétique dans l'objectif d'une gestion homogène des données. Le document poursuit l'approche des meilleures pratiques: les aspects de risque de chaque processus de traitement des données sont considérés (approche axée sur les risques). Lorsque les contenus ne sont pas directement applicables, il incombe à l'entreprise concernée de trouver une solution pertinente et conforme pour son domaine de compétence.

(3) Le présent document vise à susciter une prise de conscience quant:

- à la complexité croissante et aux défis de la gestion des données;
- à l'élaboration d'une politique des données globale, à l'échelle de l'entreprise; et
- aux possibilités qui existent en matière de gestion des données sur fond de digitalisation et de transformation numérique.

1.3 Intégration de la politique des données dans le paysage documentaire de l'AES

(1) La législation pertinente est prise en compte aussi bien dans la politique des données elle-même que dans les documents référencés dans le cadre de gestion globale.

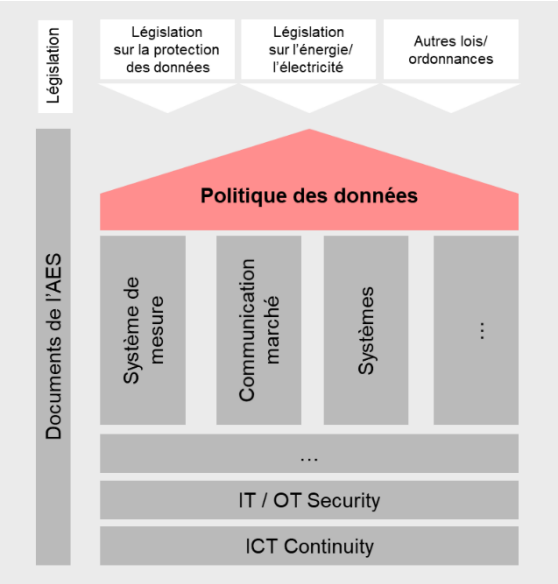


Figure 2 La politique des données, cadre pour les documents de l'AES portant sur des thèmes voisins

(2) Les documents suivants de l'AES peuvent être attribués aux différents thèmes de la figure 2:

Thème	Document
Politique des données	– Rapport sur la politique des données dans le secteur énergétique – Recommandation de la branche «Politique des données dans la branche énergétique»
Système de mesure	– Document-clé «Metering Code Suisse» – Directives pour la sécurité des données des systèmes de mesure intelligents – Manuel «Gestion des données de mesure» – Manuel «Systèmes de mesure intelligents» – Document thématique «Protection et sécurité des données dans le cadre du smart metering» – Document thématique «Responsabilité dans le domaine de la métrologie»
Communication marché	– Recommandation de la branche «Échange de données standardisé pour le marché du courant électrique CH (SDAT)» – Recommandation de la branche «Échange de données interne au groupe-bilan»
Systèmes	– Manuel «Systèmes de commande et de réglage intelligents pour l'exploitation du réseau»
IT / OT Security	– Manuel «Protection de base pour les ‹technologies opérationnelles› (OT) dans l'approvisionnement en électricité»
ICT Continuity	– Recommandation de la branche «ICT Continuity»
Décompte	– Recommandation de la branche «E-Invoicing sur le marché suisse de l'électricité»

Tableau 1 Vue d'ensemble des documents de l'AES concernés par la politique des données

2. Domaine d'application

(1) La politique des données se concentre sur les données en rapport explicite avec la branche énergétique. Les données personnelles de personnes physiques (exception: art. 17c LapEl) en font partie. Les données destinées à l'exploitation d'une organisation, sans lien direct avec la branche énergétique, ne font pas partie de la politique des données. En principe, les mêmes réflexions s'appliquent aux autres données posant des exigences de protection et de sécurité comparables (personnel, distribution, marketing, finances, etc.), mais elles ne sont pas traitées spécifiquement dans le présent document.

(2) L'élaboration et l'application d'une politique des données à l'échelle de l'entreprise constituent la base de la mise en œuvre conforme des exigences régulatoires.

3. Définitions

(1) **Politique des données**
La politique des données détermine les principes et directives en matière d'**utilisation des données**, de **conformité à la politique des données** (sécurité et protection des données) et de **gouvernance des données**. La définition de chacun de ces termes figure au début du chapitre de mise en œuvre correspondant.

(2) **Protection des données**
La finalité et l'objectif de la protection des données sont de protéger la personnalité des personnes au sujet desquelles des données sont traitées, ainsi que de garantir l'auto-détermination de l'individu en matière d'information. Chacun doit pouvoir déterminer lui-même lesquelles de ses données il rend accessibles, quand, à qui, pourquoi et pour combien de temps.

(3) **Traitement des données**
Toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données (art. 5, let. d LPD).

(4) **Communication de données**
Le fait de transmettre des données personnelles ou de les rendre accessibles (art. 5, let. e LPD).

(5) **Sécurité des données**
Ensemble des mesures techniques et organisationnelles (MTO) visant à garantir la confidentialité, la disponibilité et l'intégrité des données.

(6) **Principe du besoin de connaître (*need to know*)**
Principe selon lequel les données et informations ne sont mises à la disposition que des offices, personnes, fonctions et rôles qui en ont besoin pour leurs tâches. La mise en œuvre du principe du besoin de connaître recouvre des mesures aussi bien techniques qu'organisationnelles (MTO).

(7) **Pseudonymisation**
Mécanisme selon lequel les données personnelles d'une personne précise ne peuvent plus être associées à cette personne sans l'utilisation d'informations supplémentaires. Les données pseudonymisées restent des données personnelles, auxquelles il convient d'appliquer le droit de la protection des

données.

Un pseudonyme relie les données non modifiées à la personne. Par exemple, le pseudonyme Désignation du point de mesure établit un lien avec le client. Si l'on suit la recommandation de la branche «Metering Code CH», qui consiste à ne pas utiliser de clé logique, on peut procéder à la pseudonymisation via la désignation du point de mesure. Cf. section **Fehler! Verweisquelle konnte nicht gefunden werden.**, paragraphe (3).

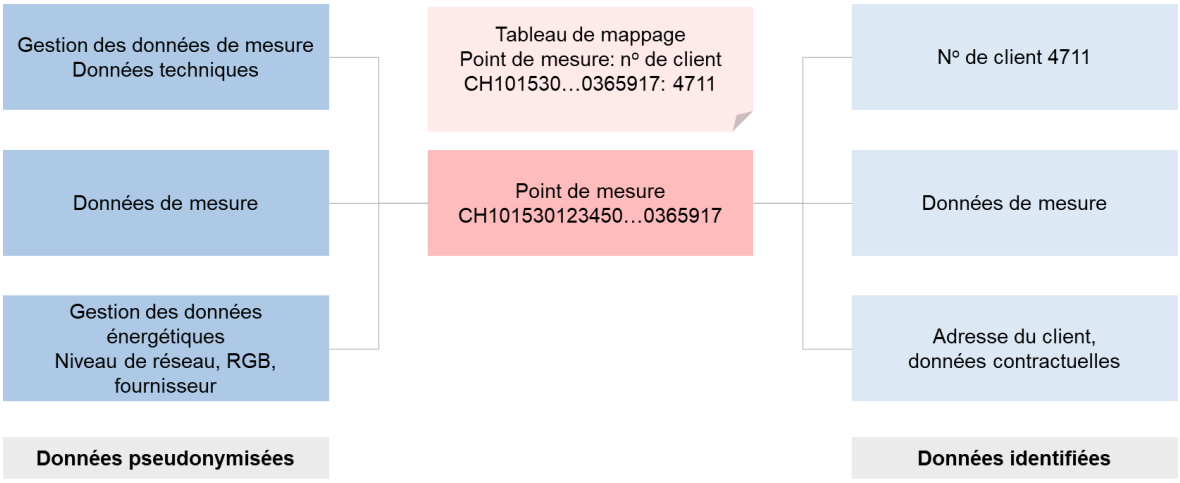


Figure 3 Exemple de mise en œuvre de la pseudonymisation avec un tableau de mappage

(8) **Anonymisation**

Modification des données personnelles de sorte que les données résultant de ce processus ne permettent plus de remonter à une personne en particulier, ou ne le permettent qu'au moyen de recherches disproportionnées. Les données ainsi générées ne sont plus des données personnelles et ne présentent pas les besoins de protection correspondants, autrement dit le droit de protection des données ne s'y applique plus. Exemples de méthodes d'anonymisation:

- Plusieurs[2] jeux de données homogènes sont agrégés: on utilise alors la somme, la moyenne arithmétique ou la médiane pour la suite du traitement.
- Toutes les informations permettant d'identifier des personnes (p. ex. nom et prénom, adresse, numéro de téléphone, adresse e-mail, objet raccordé, numéro de compteur) sont supprimées.
- Réduction de la quantité d'attributs de données.
- Facultativement, une combinaison des méthodes citées ci-avant peut être utilisée pour l'anonymisation.

[2] Le nombre exact doit être fixé en fonction de la situation, de sorte qu'il ne soit plus possible de reconnaître par déduction la personne concernée. Comme **point de repère,** on part de l'hypothèse que, lorsque 7 valeurs spécifiques / attributs / critères de sélection ou plus sont intégrés dans l'évaluation au moyen de procédés mathématiques (moyenne ou médiane arithmétique),un degré d'anonymisation suffisant peut être atteint. Il faut procéder à une vérification au cas par cas.

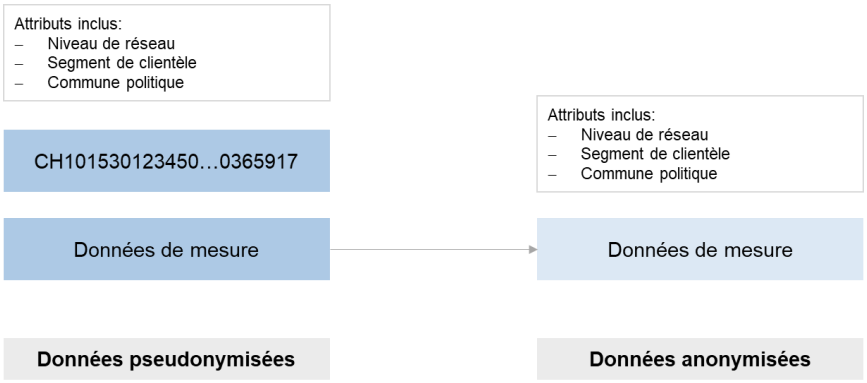


Figure 4 Exemple de mise en œuvre de l'anonymisation

(9) **Données personnelles au sein de l'EAE**
Données qui concernent une personne physique identifiée ou identifiable (art. 5, let. a LPD), et qui sont p. ex. issues de systèmes de mesure intelligents, de mesure d'installation, de programme prévisionnel et de pronostics, des signaux de commande et d'incitation, ainsi que de données clients, contractuelles ou d'électromobilité. Des informations approfondies sont disponibles au chapitre 9 «Annexe Conformité à la politique des données – modèles de données et applications».

(10) **Données non personnelles au sein de l'EAE**
Les données non personnelles sont par exemple des données relatives aux actifs, aux mandats et aux événements, et des données SCADA. Pour ce groupe de données, des exigences spécifiques à la branche s'appliquent en matière de sécurité des données. Des informations approfondies sont disponibles au chapitre 9 «Annexe Conformité à la politique des données – modèles de données et applications».

(11) **Sécurité des données («Security by Design»)**
Principe selon lequel la sécurité des données doit être prise en compte en amont, dès la phase d'élaboration des mesures techniques et organisationnelles, dans le cadre de la mise en œuvre de solutions (art. 8 LPD).

(12) **Protection des données dès la conception et par défaut («Privacy by Design/by Default»)**
Pour la protection des données personnelles, les principes s'appliquent par analogie, comme cela est décrit à la rubrique «Sécurité des données («Security by Design»)». Le Privacy by Default garantit que le respect de la vie privée est assuré dans le réglage de base des applications et des systèmes (art. 7 LPD).

(13) **Profilage («Profiling»)**
Toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique (art. 5, let. f LPD).

(14) **Profilage à risque élevé**
Tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique (art. 5, let. g LPD).

(15) **Mesures techniques et organisationnelles (MTO)**
Les MTO constituent une partie essentielle de la documentation relative à la protection des données et sont cruciales pour le registre des activités de traitement (RAT), la sous-traitance et les contrats correspondants, ainsi que pour les obligations d'information et de transparence (chapitre 11 «**Fehler! Verweisquelle konnte nicht gefunden werden.**» et art. 7, al. 2 LPD).

(16) **Remise et transmission des données personnelles (portabilité)**
Remise et transmission de données personnelles sous un format électronique couramment utilisé (art. 28, al. 1 LPD).

(17) **Analyse d'impact relative à la protection des données personnelles**
Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, il faut procéder au préalable à une analyse d'impact relative à la protection des données personnelles (art. 22, al. 1 LPD). Le responsable du traitement privé est délié de son obligation d'établir une analyse d'impact s'il est tenu d'effectuer le traitement en vertu d'une obligation légale (art. 22, al. 4 LPD, p. ex. traitement de données provenant de systèmes de mesure intelligents ainsi que données énergétiques dans l'approvisionnement de base selon OApEl).

(18) **Registre des activités de traitement**
Compilation des activités de traitement en fonction des processus (art. 12 LPD). Cf. à ce sujet la section 8.3 «Registre des activités de traitement».

(19) **Responsable du traitement**
La personne privée (au sens de personnes physiques et morales) ou l'organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles (art. 5, let. j LPD).

(20) **Sous-traitant**
La personne privée (au sens de personnes physiques et morales) ou l'organe fédéral qui traite des données personnelles pour le compte du responsable du traitement (art. 5, let. k LPD).

4. Vue d'ensemble de la mise en œuvre de la politique des données

(1) La mise en œuvre des exigences régulatoires et juridiques ainsi que de la politique des données par une EAE nécessite une série d'étapes de travail afin de prendre en compte tous les aspects relatifs aux données. Pour une mise en œuvre efficace, un changement de culture à l'échelle de l'entreprise, avec des mesures incluant tous les niveaux hiérarchiques et menées par le conseil d'administration et la direction, est recommandé.

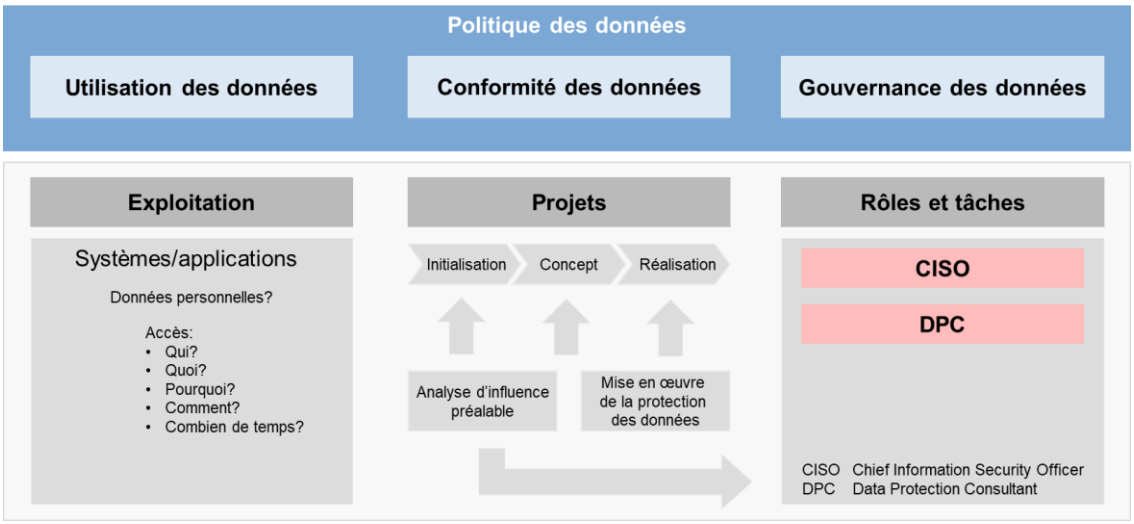


Figure 5 Thèmes abordés dans le cadre de la mise en œuvre de la politique des données

(2) Il convient alors, pour une gestion homogène des données, de définir clairement les rôles et responsabilités au sein de l'entreprise. Le chapitre 8 «Recommandations de mise en œuvre en matière de gouvernance des données» décrit les rôles et/ou fonctions importants qui doivent être attribués et assumés.

(3) À partir des processus, d'une vue d'ensemble des flux de données et d'un inventaire des données, il est recommandé d'établir un «registre des activités de traitement» (RAT) conformément à la section 8.3, ainsi qu'un registre de l'infrastructure TIC, qui constitueront des éléments-clés pour déterminer la gestion correcte des données.

(4) Dans le cadre de la réalisation de projets (concepts, modifications, etc.), par exemple pour la conception de services et de processus commerciaux, la gestion des données doit être fixée en amont. Il convient de prendre en compte:

- les exigences envers la protection des données (p. ex. analyses d'impact relatives à la protection des données (AIPD), «Privacy by Design/by Default»);
- les exigences en matière de sécurité des données (p. ex. «Security by Design»);
- la garantie des droits des personnes concernées (p. ex. renseignements, ainsi que rectification, blocage et suppression des données);
- les exigences en matière d'utilisation des données concernant les conditions-cadre régulatoires.

La satisfaction de toutes les exigences relatives aux données doit être garantie au moment de la clôture du projet. Le chapitre 7 «Recommandations de mise en œuvre en matière de conformité à la politique des données» décrit les bases y relatives.

(5) L'ensemble du cycle de vie doit être pris en compte lors de la définition de la gestion des données: leur acquisition, leur stockage, leur conservation, leur utilisation, leur modification, leur publication, leur archivage, leur suppression et leur destruction.

(6) Toute forme de données doit, en principe, être classée dans une catégorie et protégée en conséquence, et l'utilisation des données conforme au droit doit être garantie. L'utilisation correcte des données, et ce dans le respect des directives relatives à la gestion des données personnelles ou non

personnelles, doit être garantie en tout temps. En outre, il convient de garantir les droits des personnes concernées. Les bases relatives au thème de l'utilisation des données sont exposées au chapitre 6 «Recommandations de mise en œuvre en matière d'utilisation des données».

(7) Le traitement des données personnelles doit être explicable à tout moment et concorder avec les dispositions relatives à la législation sur la protection des données correspondante. Les collaborateurs doivent connaître les règles.

(8) Un guide sur les principaux éléments de mise en œuvre figure au chapitre 13.

5. Fondements juridiques

(1) Le présent document n'aborde pas les éventuelles réglementations plus détaillées figurant dans les lois cantonales sur la protection des données.

(2) Du point de vue spécifique à la branche, les régulations relatives à l'utilisation des données issues de la séparation au niveau de l'information sont, conformément à l'art. 10, al. 2 LApEl, cruciales pour un accès au réseau non discriminatoire et pour la préservation de la concurrence. Pour de plus amples explications, cf. section 6.1 «Séparation («Unbundling»)».

(3) Pour le traitement des données de mesure en lien avec les systèmes de mesure, de commande et de réglage intelligents, ce sont les prescriptions légales spécifiques selon l'art. 8d OApEl qui s'appliquent. Ces prescriptions priment les réglementations fédérales et cantonales relatives à la protection des données. Pour de plus amples explications, cf. section 7.3 «Traitement des données de mesure conformément à l'OApEl».

5.1 Vue d'ensemble des réglementations, des lois et des normes ainsi que des limitations

(1) Le présent document aborde les conditions-cadre du marché de l'électricité pour la branche énergétique et les secteurs apparentés. Il s'agit des textes suivants:

Réglementation	Abréviation
Loi sur l'énergie	LEne
Ordonnance sur l'énergie	OEne
Loi sur l'approvisionnement en électricité	LApEl
Ordonnance sur l'approvisionnement en électricité	OApEl
Loi fédérale sur la protection des données du 25 septembre 2020	LPD
Lois cantonales sur la protection des données	-
Ordonnance relative à Loi fédérale sur la protection des données	OLPD
Règlement général de l'Union européenne sur la protection des données	RGDP
Ordonnance concernant la tenue et la conservation des livres de compte	Olico

Tableau 2 Vue d'ensemble des réglementations

(2) L'applicabilité du RGPD pour les EAE suisses peut être établie dans les trois situations suivantes:

– lorsque l'EAE a une succursale dans l'UE;

– lorsque l'EAE propose des biens ou des services dans l'UE;

– lorsque l'EAE observe le comportement de ses clientes et clients dans l'UE afin de leur soumettre des offres personnalisées.

cf. aussi chapitre 12 «Annexe FAQ RGPD».

(3) Le présent document se concentre exclusivement sur le domaine d'application décrit au chapitre 2.

5.2 Données personnelles

(1) Les législateurs en Suisse et dans l'UE ont établi une définition descriptive qui n'est pas exhaustive dans la pratique.

(2) Loi fédérale sur la protection des données (LPD), art. 5, let. a:
Données personnelles (données): toutes les informations qui se rapportent à une personne physique identifiée ou identifiable.

(3) On peut en déduire qu'il existe des données qui peuvent être attribuées de façon explicite à une certaine personne (p. ex. nom, prénom, date de naissance, adresse). La définition comprend aussi toute forme de données permettant d'identifier une personne (p. ex. par une analyse des données, un profilage). Mais cette possibilité d'identification peut aussi découler de données quelconques. De telles données sont également soumises à la protection des données si l'identification d'une personne physique découle du contexte.

(4) Les applications commerciales courantes dans le cadre desquelles un lien personnel (personne identifiée) ou indirect (personne identifiable) est établi ou peut être établi sont notamment:

- la gestion de la relation client (Customer Relationship Management, CRM);
- la documentation relative aux installations et aux bâtiments, p. ex. les données SIG complétées avec des informations personnelles;
- les systèmes de données de mesure;
- la gestion des documents, p. ex. contrats, servitudes;
- le progiciel de gestion intégrée (Enterprise Resource Planning, ERP);
- les systèmes de comptabilité et de décompte en lien avec l'énergie avec des données clients, créditeurs et débiteurs;
- les solutions utilisant des processus analytiques pour les catégorisations, les segmentations, les groupements, l'agrégation («Clustering»), la cotation («Scoring»), etc.

5.3 Données personnelles particulièrement sensibles

(1) Il existe également des données personnelles particulièrement sensibles. Celles-ci ne peuvent en principe être collectées et stockées que si elles sont pertinentes pour l'activité commerciale de l'EAE. En général, de telles données figurent dans les activités de base d'une EAE. Les cas particuliers sont à évaluer séparément.

(2) La Loi fédérale sur la protection des données définit à l'art. 5, let. c, les données correspondantes. Les données personnelles particulièrement sensibles sont soumises à des restrictions supplémentaires.

(3) On peut en déduire les catégories particulièrement sensibles suivantes:

Catégorie
Positions et activités religieuses, idéologiques, politiques, syndicales
Données relatives à la santé, à la sphère intime, à la race, à l'ethnie
Mesures d'aide sociale
Poursuites et sanctions administratives et pénales
Données génétiques
Données biométriques qui identifient clairement une personne physique

Tableau 3 Catégories de données personnelles particulièrement sensibles

5.4 Profilage et profilage à risque élevé

(1) Lors du recours au profilage (cf. paragraphes (13) et (14) du chapitre 3 «Définitions»), des mesures techniques et organisationnelles appropriées aux besoins de protection doivent être prises. En cas de profilage à risque élevé, il faut réaliser une analyse d'impact relative à la protection des données pour clarifier les besoins de protection, et, dans le domaine du droit public, établir en plus un règlement pour le traitement.

(2) Dans le cadre de cette politique des données, la thématique est notamment pertinente dans le domaine du Smart Metering (p. ex. conformément à l'art. 17c LApEl en lien avec l'art. 8d OApEl «Traitement des données enregistrées au moyen de systèmes de mesure, de commande et de réglage intelligents»).

5.5 Traitement des données

(1) Le concept de traitement des données provient des législations sur la protection des données de la Suisse et de l'UE.

(2) Le traitement recouvre toutes les actions et activités en lien avec les données et informations, peu importent :

a. les médias qui sont utilisés (p. ex. informatique, papier);
b. la manière dont elles sont effectuées: active (p. ex. saisie) ou passive (p. ex. consultation);
c. la phase du cycle de vie dans laquelle elles se trouvent (phase 1: génération/fourniture/création, phase 2: utilisation/traitement, phase 3: conservation/archivage/suppression).

Cf. à ce sujet le chapitre 3, paragraphe (3).

(3) La forme revêtue par ces actions et activités ainsi que les conditions dans lesquelles elles sont effectuées (p. ex. par des personnes, un ordinateur, l'entité juridique propre ou des tiers, en Suisse ou à l'étranger) n'ont que peu d'importance.

(4) Une source centrale, consignant l'ensemble des activités de traitement des données en fonction des processus, est essentielle pour assurer le bon traitement des données (LPD: art. 12, Registre des activités de traitement).

(5) Par ailleurs, les données sont soumises à d'autres restrictions régulatoires, telles que les directives relevant du droit de la concurrence et des cartels (p. ex. séparation des activités conformément à la

LApEl et à l'OApEl) ainsi que les dispositions sur le secret de fonction et/ou d'affaires. Les mêmes données que celles qui sont pertinentes pour la protection des données peuvent alors être concernées.

5.6 Sous-traitance de données

(1) Lorsque des données personnelles sont traitées par des tiers (entité juridique différente), une réglementation contractuelle au sens de la sous-traitance selon l'art. 9, al. 1 LPD est nécessaire (les exceptions sont à considérer au cas par cas, p. ex. lorsqu'une base légale existe pour la transmission de données). Le responsable détermine la finalité du traitement et la manière dont il est effectué, et définit les mesures techniques et organisationnelles (MTO) requises. Ces prescriptions s'appliquent aussi aux partenaires contractuels des sous-traitants. La responsabilité incombe toutefois toujours au donneur d'ordre (le responsable, selon la LPD) et les obligations de contrôle correspondantes lui reviennent donc également (cf. art. 9, al. 2 LPD).[3]

(2) Là où plusieurs entités juridiques forment une entité économique, p. ex. des groupes ou des structures de droit public, une analyse et une réglementation détaillées sont nécessaires. Sur le principe, il n'existe toujours pas de «privilège de groupe». En matière de protection des données, les sociétés d'un groupe doivent être considérées comme des sociétés séparées et indépendantes.

(3) Le fait de recourir à des tiers pour le traitement des données doit être communiqué aux personnes concernées dans le cadre des obligations de transparence et d'information sous une forme générale, soit sans obligatoirement citer de noms (p. ex. dans la déclaration de confidentialité).

(4) Les domaines d'application typiques sont par exemple: l'utilisation générale du cloud, l'utilisation de centres informatiques externes, l'externalisation de processus commerciaux tels que les prestations de services de mesure, le recours à des portails, à des boutiques en ligne ou assimilés, et leur utilisation.

5.7 Gestion des données des personnes morales

(1) Les données des personnes morales ne sont pas soumises à la LPD suisse (demeurent réservées les prescriptions plus détaillées figurant dans les lois cantonales sur la protection des données). Toutefois, la LPD s'applique par analogie aux données provenant de systèmes de mesure, de commande et de réglage intelligents appartenant à des personnes morales (art. 17c, al. 1 LApEl)[4].

6. Recommandations de mise en œuvre en matière d'utilisation des données

(1) Les recommandations de mise en œuvre en matière d'utilisation des données recouvrent des thèmes importants pour le traitement et la prise en compte des droits d'utilisation des données.

(2) Si des services sont fournis (y c. traitement et stockage des données) à des clients sur le territoire suisse, la législation suisse s'applique en principe. Dans tous les autres cas, les dispositions régulatoires (étrangères) complémentaires s'appliquent. Cf. section 5.1, paragraphe (2).

[3] Mesures techniques et organisationnelles de la protection des données PFPDT: https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/dokumentation/guides/mesures-techniques-et-organisationnelles-de-la-protection-des-do.html
[4] Source: https://www.fedlex.admin.ch/eli/fga/2020/1998/fr, p. 70

6.1 Séparation («Unbundling»)

(1) La séparation des activités au niveau de l'information («Unbundling») désigne la distinction entre l'exploitation du réseau et les autres secteurs d'activité d'une EAE (art. 10, al. 2 LApEl: «*Sous réserve des obligations de renseigner prévues par la loi, les informations économiques sensibles obtenues dans le cadre de l'exploitation des réseaux électriques doivent être traitées confidentiellement et ne pas être utilisées dans d'autres secteurs d'activité par les entreprises d'approvisionnement en électricité*.»). Les autres secteurs d'activité peuvent être p. ex. la vente d'énergie sur le marché libre, le conseil en énergie, l'installation ou le passage de contrats («Contracting»).

(2) Dans le cadre de la libéralisation partielle du marché de l'électricité, des structures concurrentielles ont été créées par le biais de la séparation des activités et un accès au réseau non discriminatoire pour les tiers a été assuré. La séparation au niveau de l'information doit empêcher l'utilisation non autorisée d'informations issues du monopole naturel pour les activités sur le marché libre, de façon à éviter tout avantage concurrentiel dans les secteurs d'activité d'une EAE en dehors du monopole naturel et, ainsi, de protéger la concurrence. Un avantage concurrentiel non autorisé vis-à-vis d'autres acteurs du marché peut être dû à:

- une baisse des dépenses;
- une avance temporelle;
- un revenu supplémentaire.

(3) Les dispositions de séparation des activités visent non pas à protéger les données, mais à préserver une concurrence juste. Il faut garantir que, dans le cadre d'une activité de marché, aucun participant au marché n'est favorisé ou ne peut profiter d'une position privilégiée (principe des règles du jeu identiques pour tous les acteurs du marché). Les données doivent ainsi être considérées du point de vue de la séparation des activités et de la neutralité de la concurrence, en plus de celui de la sécurité et de la protection, et traitées en conséquence.

(4) Bien que, dans certains cas, une utilisation des données serait possible du point de vue du droit de la protection des données, les prescriptions sur la séparation des activités au niveau de l'information peuvent l'interdire. L'utilisation des données dans le cadre de la séparation au niveau de l'information doit toujours être évaluée concrètement au cas par cas.

6.2 Utilisation des données issues de l'exploitation du réseau et de l'approvisionnement de base

(1) Le principe suivant s'applique: les données des utilisateurs du réseau dont un gestionnaire de réseau a connaissance en raison de l'exploitation de ce dernier et de l'exécution du mandat d'approvisionnement de base ne peuvent pas être utilisées pour des activités concurrentielles. Il faut prendre des mesures afin de garantir le respect des prescriptions de séparation des activités (p. ex. mesures techniques et organisationnelles [MTO], formations, instructions sur la façon de procéder, etc.).

(2) Les données des utilisateurs du réseau sont en général des **informations économiquement sensibles**, car le gestionnaire de réseau peut se ménager un avantage concurrentiel avec les informations obtenues (art. 10, al. 2 LApEl). Parmi elles, on compte:

- le nom, l'adresse et d'autres données de base;
- les données de consommation obtenues à partir de systèmes de mesure, de commande et de réglage intelligents;

- les métadonnées et données structurelles en rapport, telles que les informations pertinentes pour la maintenance.

Une utilisation des données en dehors de l'exploitation du réseau et de l'approvisionnement de base par l'EAE ou par des tiers, ainsi que, le cas échéant, la transmission à des tiers sont notamment possibles s'il existe un accord explicite ad hoc. Celui-ci ne peut cependant pas être obtenu et traité sur la base d'informations et de ressources issues de l'exploitation du réseau ou de l'approvisionnement de base (cf. section 6.1 Séparation («Unbundling»), paragraphes (1) et (2)). Il y a par exemple accord si un client transmet lui-même les données à l'EAE ou à des tiers.

(3) En principe, les données déterminantes pour le décompte et la rétribution (cf. définition à la section 7.3 «Traitement des données de mesure conformément à l'OApEl») ne sont pas pseudonymisées dans:

- les systèmes destinés au décompte de l'utilisation du réseau, de l'énergie, des taxes, du supplément sur les coûts de transport du réseau à haute tension;
- les rétributions pour l'utilisation des systèmes de commande et de réglage.

L'attribution des données personnelles (notamment les courbes de charge de 15 minutes) au client correspondant n'est modifiable que par les personnes autorisées (en interne ou en externe) exécutant des processus pertinents pour le décompte et la rétribution. Cf. chapitre 10 «Annexe Conformité à la politique des données – données issues de l'exploitation du réseau et de l'approvisionnement de base».

(4) Conformément à la LApEl, les dispositifs de mesure seront transformés en systèmes de mesure intelligents dans les prochaines années. Dans la mesure où les valeurs de courbe de charge ou les valeurs de registre sont pertinentes pour le décompte, ces données peuvent être utilisées sous forme non pseudonymisée à des fins de décompte, de rétribution et de visualisation de la consommation (art. 8a, al. 2, let. c en lien avec l'art. 8d, al. 1, let. b OApEl). La transmission de données de courbe de charge vers les systèmes de facturation doit se faire, dans la mesure du possible, sous forme agrégée. Exemple: si une valeur mensuelle est nécessaire pour le décompte, il faut reporter, depuis le système de gestion des données de mesure ou des données énergétiques, vers le système de décompte, une somme mensuelle agréée issue des données de courbe de charge ou la valeur de registre correspondante.

(5) Si les courbes de charge sont visualisées par les utilisateurs du réseau, la pseudonymisation dans le système d'affichage doit être réduite de façon à ce que seules les courbes de charge ou d'injection autorisées puissent être représentées de façon compréhensible pour l'utilisateur du réseau.

(6) Pour les données dans le système-test, les mêmes exigences que pour un système productif s'appliquent, peu importe que les données soient à jour ou non.

6.3 Utilisation des données issues de systèmes de mesure intelligents de l'EAE

(1) L'utilisation de données provenant de systèmes de mesure intelligents se voit poser des limites légales étroites. Sans l'accord du client final, les gestionnaires de réseau ont le droit de traiter les données à des fins de visualisation de la consommation selon art. 8a, al. 2, let. c OApEl, ainsi qu'à des fins de décompte et pour garantir l'exploitation du réseau selon art. 8d OApEl.

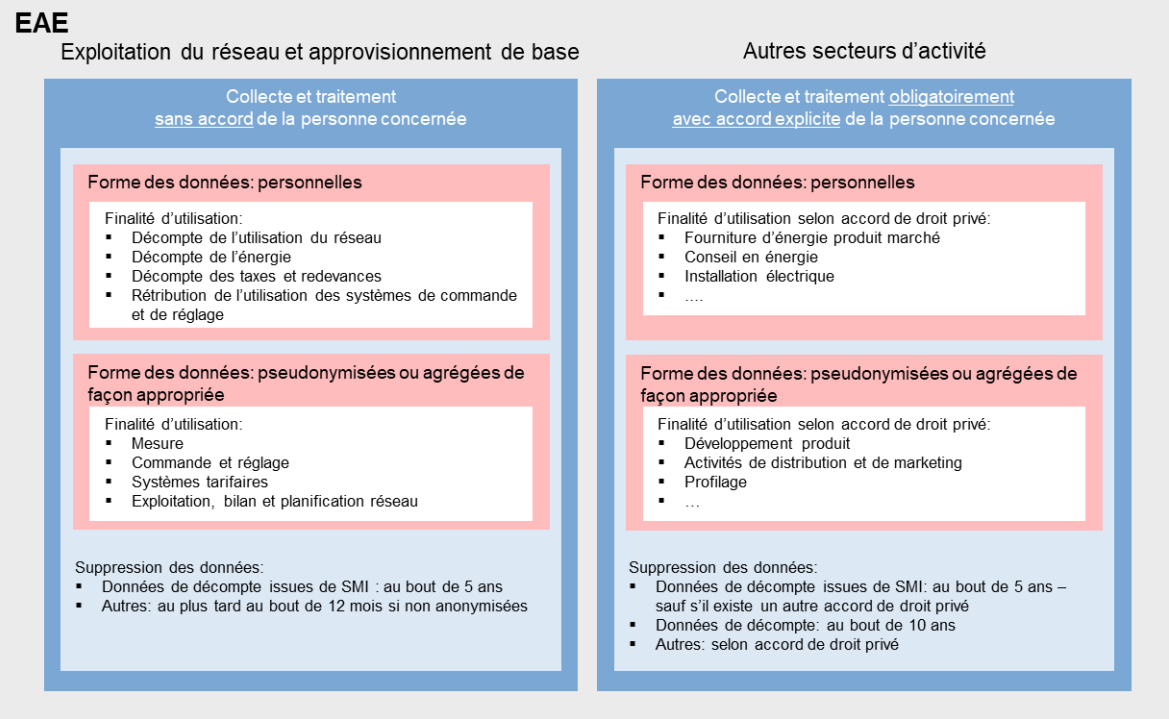


Figure 6 Utilisation des données issues de SMI (art. 8d OApEl) en lien avec la séparation au niveau de l'information (art. 10, al. 2 LApEl)

(2) Une utilisation des données plus étendue que les domaines d'application définis dans les art. 8a, al. 2, let. c et art. 8d OApEl n'est possible qu'avec l'accord explicitement obtenu du client final (*opt-in*). Pour obtenir l'accord explicite du client final sur l'utilisation des données, seules peuvent être utilisées – hors de l'exploitation du réseau et de l'approvisionnement de base – les données (d'adresse) qui ne proviennent pas de l'exploitation du réseau ni de l'approvisionnement de base (p. ex. données d'adresse achetées)[5]. Une finalité d'utilisation définitive doit être indiquée au client final lorsque l'on demande son accord explicite. Pour les clients finaux à l'approvisionnement de base, cela ne peut pas être réglé via les conditions générales. L'accord explicite doit pouvoir être prouvé.

6.4 Implication de tiers

(1) Si une entreprise achète des services de tiers, il convient de s'assurer que ces derniers respectent la protection et la sécurité des données ainsi que d'autres dispositions régulatoires pertinentes (pour les contrats existants et nouveaux). Les tiers (cf. section 5.6 «Sous-traitance de données»**Fehler! Verweisquelle konnte nicht gefunden werden.**) sont p. ex. des fournisseurs de données de mesure mandatés par le gestionnaire de réseau de distribution (GRD), des techniciens chargés du décompte énergétique, des gestionnaires de plateformes de données, des gestionnaires de systèmes de cloud, des administrateurs système d'un partenaire d'externalisation et des collaborateurs support d'un concepteur de logiciels. Toute entité juridique différente de l'entité juridique qui collecte/traite les données doit être considérée comme un tiers du point de vue du droit de la protection des données. En principe, cela s'applique également au sein des groupes de sociétés.

[5] cf. section 6.2 **Fehler! Verweisquelle konnte nicht gefunden werden.**

7. Recommandations de mise en œuvre en matière de conformité à la politique des données

(1) La conformité à la politique des données[6] dans la branche énergétique recouvre le respect des lois, ordonnances, documents de la branche et directives internes, notamment du point de vue de la collecte, du traitement, de la transmission et de l'utilisation des données. Le traitement constitue alors un concept global de saisie, de stockage, de suppression, de modification, de sauvegarde, de transfert, de consultation, d'évaluation, etc. La conformité à la politique des données dans la branche énergétique est surtout considérée du point de vue de la protection des données, de la sécurité des données et de la séparation des activités.

- La protection des données préserve la sphère privée des personnes. Elle doit permettre et garantir l'auto-détermination en matière d'information dans la gestion des données et informations pertinentes.
- La sécurité des données désigne les exigences et mesures visant à garantir la sécurité physique et logique nécessaire des données et informations.
- Les fondements juridiques déterminants pour la garantie de la conformité à la politique des données sont notamment l'Ordonnance sur l'approvisionnement en électricité (art. 8 et 8d OApEl) et l'Ordonnance relative à la Loi fédérale sur la protection des données (OLPD).
- Les fondements de la garantie de la conformité à la politique des données sont décrits au chapitre 6 du rapport de l'AES sur la politique des données dans le secteur énergétique (2018). Des mesures techniques et organisationnelles y sont présentées.
- La protection et la sécurité des données se conditionnent mutuellement.

(2) L'application de la conformité à la politique des données prend en compte les conditions-cadre des différentes EAE (taille et organisation de l'entreprise, secteurs d'activité, etc.).

7.1 Protection des données

(1) Les exigences légales de la législation sur la protection des données concernant les données personnelles nécessitent une mise en œuvre dans l'entreprise, sous la forme d'instructions, de directives, de check-lists, de manuels, etc.

(2) Pour mettre en œuvre et garantir la protection des données nécessaire, il convient d'examiner les données personnelles identifiées dans le cadre de l'utilisation des données au regard des besoins de protection, du traitement conforme, de l'utilisation et de la transmission. En outre, les mesures techniques et organisationnelles (MTO) qui s'imposent doivent être définies et mises en œuvre. Les informations correspondantes sont notamment consignées dans le registre des activités de traitement (RAT). Cf. à ce sujet la section 8.3 «Registre des activités de traitement».

(3) Une analyse complète de la protection des données recouvre toutes les données, et donc aussi celles qui n'ont pas de lien particulier avec la branche énergétique. Il s'agit p. ex. de données collaborateurs (rapports d'accident, certificats médicaux, entre autres), de données clients et fournisseurs, de la comptabilité, des contrats, de l'inventaire, des documentations processus, des procédures et opérations, des mandats, des factures et du secret d'exploitation. Conformément au paragraphe (5)**Fehler! Verweisquelle konnte nicht gefunden werden.** de la section 5.5 «Traitement

[6] Aussi appelée «compliance»

des données», diverses bases légales s'appliquent aux données citées. En principe, toutes les données personnelles doivent être saisies et consignées dans le registre des activités de traitement (RAT). Cf. à ce sujet la section 8.3 «Registre des activités de traitement».

(4) L'évaluation, l'accumulation et la combinaison de données peuvent en particulier entraîner la création de nouvelles ou d'autres données personnelles; c'est la raison pour laquelle il faut vérifier au préalable la nécessité d'évaluer les risques de manière systématique (analyse d'impact relative à la protection des données personnelles). Plusieurs modèles à cet effet sont disponibles sur Internet.

(5) Une analyse d'impact relative à la protection des données personnelles doit être réalisée préalablement à un traitement de données personnelles présentant un risque élevé pour la personnalité ou pour les droits fondamentaux des personnes concernées, sous la forme d'une évaluation détaillée des risques, pour le processus de traitement des données (exceptions: cf. art. 22 LPD).

7.2 Sécurité des données

(1) Pour garantir la sécurité des données, les exigences et mesures nécessaires doivent être identifiées. À cet effet, il convient dans un premier temps de définir les besoins de protection des objets de données. Des mesures en seront déduites dans un second temps. Cf. à ce sujet la section 6.2 du rapport de l'AES sur la politique des données dans le secteur énergétique (2018).

(2) Pour tous les objets de données, une analyse CIA et une détermination sur la base du RAT sont réalisées.

- C = Confidentiality = Confidentialité
- I = Integrity = Intégrité
- A = Availability = Disponibilité

De plus, les objets de données doivent aussi être évalués concernant les éléments suivants:

- A = Authentication = Authentification
- A = Authorization = Autorisation
- A = Accounting = Traçabilité

Il en résulte une analyse CIA-AAA complète.

7.3 Traitement des données de mesure conformément à l'OApEl

Pour avoir une meilleure vue d'ensemble, le traitement des données de mesure conformément à l'OApEl est récapitulé dans le graphique suivant.

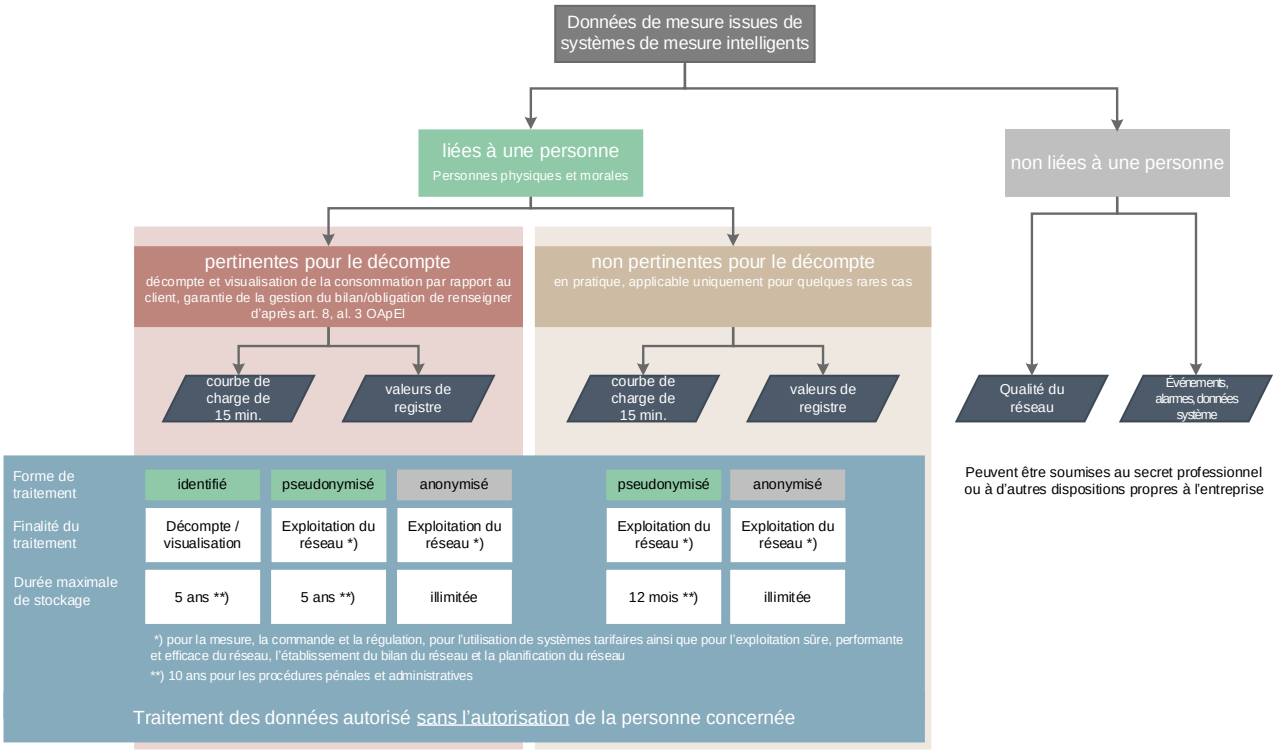


Figure 7 Traitement des données de mesure conformément à l'OApEl

7.3.1 Traitement des données de mesure liées à une personne (données pertinentes pour le décompte)

(1) Conformément à l'art. 17c LApEl, la Loi sur la protection des données s'applique aux traitements de données personnelles en lien avec des systèmes de mesure, de commande et de réglage intelligents. Cette réglementation vaut aussi pour les données de mesure liées à une personne aussi bien les données personnelles que les données de personnes morales. Les données de mesure liées à une personne peuvent être traitées et conservées de la façon suivante, peu importe qu'il s'agisse de données de courbe de charge (avec un intervalle de 15 minutes maximum) ou de valeurs de registre.

- D'après l'art. 8d, al. 3 OApEl, les données doivent être détruites après douze mois ou anonymisées, sauf si elles sont pertinentes pour le décompte ou qu'elles servent à la visualisation pour le client.
- Les données sont pertinentes pour le décompte si elles sont utilisées pour établir des décomptes et pour garantir la gestion du bilan ou l'obligation de renseigner selon l'art. 8, al. 3 et 4 OApEl.
- Les données pertinentes pour le décompte ou qui servent à la visualisation pour le client peuvent être traitées sans l'autorisation des clients concernés, sous forme non pseudonymisée (c.-à-d. sous une forme où la personne est identifiée, d'après art. 8d, al. 1, let. b OApEl) et conservées jusqu'à 5 ans (art. 8, al. 4 OApEl: «*Tous les chiffres relevés au cours des cinq années précédentes doivent être livrés.*»). Les données doivent ensuite être supprimées ou transformées en une forme anonymisée appropriée ou en un agrégat approprié (cf section 7.1).

- Les données visant à garantir l'exploitation du réseau (selon art. 8d, al. 1, let. a OApEl) peuvent être traitées sous forme pseudonymisée sans l'autorisation des clients concernés et conservées jusqu'à 5 ans.
- Les données provenant de procédures pénales ou administratives, ainsi que la facture d'électricité proprement dite doivent être conservées pendant 10 ans (art. 70 OEne).
- Pour pouvoir conserver plus longtemps des données, il faut avoir l'autorisation expresse du client.

7.3.2 Traitement des données de mesure liées à une personne (données non pertinentes pour le décompte)

(1) Conformément à l'art. 8d, al. 3 OApEl, ces données (p. ex. pour garantir l'exploitation sûre du réseau) doivent être détruites après douze mois ou anonymisées.

- Elles peuvent être sous forme pseudonymisées sans l'autorisation des clients concernés et conservées jusqu'à 12 mois.
- Les données provenant de procédures pénales ou administratives doivent être conservées pendant 10 ans (art. 70 OEne).
- Pour pouvoir conserver plus longtemps des données, il faut avoir l'autorisation expresse du client.

7.3.3 Traitement des données de mesure non liées à une personne

(1) Sont considérées comme données de mesure non liées à une personne les événements, alarmes, données PQ, etc.

- Elles peuvent être traitées et conservées indéfiniment.
- Ces données peuvent être soumises au secret professionnel ou à d'autres dispositions internes à l'entreprise.

7.3.4 Autres dispositions

(1) Données anonymisées

- Les données anonymisées peuvent être traitées et conservées indéfiniment (cf. chapitre 3 «Définitions»). Dans ce cas, les données ne peuvent toutefois plus être utilisées pour satisfaire à l'obligation de renseigner d'après l'art. 8, al. 4 OApEl, car il n'est plus possible de les attribuer à un utilisateur du réseau.

(2) OApEl: art. 8 Système de mesure et processus d'information, al. 4:
«Sur demande et contre un dédommagement couvrant les frais, les gestionnaires de réseau fournissent des données et informations supplémentaires aux responsables de groupes-bilan ainsi qu'aux autres acteurs concernés, avec l'accord des consommateurs finaux ou des producteurs concernés. Tous les chiffres relevés au cours des cinq années précédentes doivent être livrés.»

- Il faut avoir l'autorisation de l'utilisateur du réseau pour transmettre des données et informations supplémentaires.

(3) Les entreprises doivent assurer une gestion du cycle de vie pour toutes les bases de données. Cela inclut p. ex. la saisie/collecte, le traitement, la conservation, l'archivage, la suppression, le renseignement (cf. aussi section 5.5 «Traitement des données», paragraphe (3).

7.4 Gestion approfondie des données personnelles

(1) Pour toute forme d'utilisation approfondie des données, p. ex. pour la publication ou la transmission de données, il faut en principe faire la distinction entre les données issues de l'activité au sein de l'approvisionnement de base (rapport contractuel relevant du droit public) et les données issues de l'activité hors de l'approvisionnement de base (rapport contractuel relevant du droit privé). L'absence d'alternative pour les clients captifs est alors déterminante.

- **Données issues de l'activité au sein de l'approvisionnement de base**: les données traitées dans le cadre de l'approvisionnement de base ne doivent en principe pas être réutilisées à d'autres fins. Si ces données sont utilisées à des fins sortant de l'approvisionnement de base, il faut se les procurer séparément sur le marché libre (pour éviter les distorsions de concurrence).
- **Données issues de l'activité hors de l'approvisionnement de base**: la réutilisation de données hors de l'activité d'approvisionnement de base doit être réglée par contrat (p. ex. par un accord explicite ou implicite du client). Une réglementation correspondante dans les CGV prenant en compte les directives contraignantes de la Loi fédérale sur la protection des données ainsi que la séparation des activités conformément à la LApEl est **suffisante** du point de vue juridique.
  L'art. 8d OApEl, en vigueur depuis le 1er janvier 2018, décrit l'objectif d'utilisation primaire pour lequel aucun accord des personnes concernées n'est nécessaire. Les personnes autorisées à transmettre les données sont également définies. Cette transmission des données doit au moins prendre une forme pseudonymisée. La transmission des informations pour le décryptage du pseudonyme s'effectue toujours séparément et seulement à destination des personnes disposant d'une autorisation ad hoc (p. ex. pour la fourniture de données de livraison au fournisseur d'énergie).

(2) La remise et la transmissibilité de données d'après l'art. 8a, al. 2, let. c OApEl vise à permettre aux personnes ou clients concernés, outre une visualisation, l'accès à leurs données de mesure relevées toutes les 15 minutes au cours des 5 dernières années ainsi que leur téléchargement, gratuitement et dans un format de données courant à l'échelle internationale (p. ex. au format .csv ou .xml).

(3) La remise et la transmission d'après l'art. 28 LPD vise à ce que, dans le cas d'un traitement automatisé des données, la personne concernée ait le droit de demander au responsable du traitement la remise de ses données personnelles dans un format électronique courant. Cela vaut également pour les contrats existants ou ébauchés. La personne concernée peut aussi demander une transmission de ses données à un autre responsable du traitement si cela n'engendre pas de charge disproportionnée.

(4) Dans le cadre d'un traitement des données en dehors de l'entité juridique propre (tiers ou autre entité juridique au sein d'un groupe), les fondements juridiques spécifiques doivent être pris en compte.

(5) Si des données personnelles sont communiquées à l'étranger, la personne doit en être informée lors de leur acquisition, avec mention de l'État. Il faut alors prêter attention aux territoires et espaces (cf. espace virtuel sur Internet, cloud, utilisation). Si le pays ne dispose pas d'une législation adéquate

sur la protection des données[7] et que le niveau nécessaire ne peut pas non plus être garanti d'une autre façon, il faut en outre recueillir l'accord explicite du client et prendre des mesures techniques et organisationnelles complémentaires. Cf. à ce sujet l'art. 17, al. 1, let. a LPD.

(6) Pour la conservation et l'archivage des données, les dispositions pertinentes doivent être respectées conformément à l'Ordonnance concernant la tenue et la conservation des livres de compte et à diverses autres réglementations juridiques spécifiques. Cela comprend notamment des directives relatives à la sécurité de la révision et à la durée de conservation. Il existe par ailleurs une obligation de conservation des données de metering pour l'exploitant réseau conformément à l'OApEl. Cf. à ce sujet la section 7.3 «Traitement des données de mesure conformément à l'OApEl».

(7) La personne concernée a le droit d'obtenir des renseignements sur ses données traitées. Le préposé fédéral à la protection des données met un formulaire standard (demande d'accès simple) à disposition. Il faut en principe répondre aux demandes de renseignements gratuitement dans les 30 jours. Dans certains cas, les personnes peuvent exiger une régularisation, un blocage ou une suppression de leurs données. Des droits et obligations supérieurs sur le plan juridique et régulatoire restent réservés.

7.5 Gestion des données non personnelles (sans lien direct avec des personnes)

(1) **Données d'actifs et SIG**
Les directives de l'Ordonnance sur les lignes électriques (OLEI) doivent être respectées (p. ex. la réglementation spécifiant quelles informations doivent être consultables par le public). Il reste à déterminer dans quelle mesure la documentation d'infrastructures critiques, telles que des centrales nucléaires, des installations militaires et des hôpitaux, doit faire l'objet d'une protection particulière.

(2) **Données de commande et d'événements**
Si des personnes physiques ou morales (art. 17c LApEl) sont concernées, la législation sur la protection des données s'applique et la gestion des données doit s'effectuer conformément aux directives correspondantes dans la mesure où ces données proviennent de systèmes de mesure, de commande et de réglage intelligents. À ce sujet, cf. aussi section 5.7 «Gestion des données des personnes morales».

(3) **Données SCADA**
Si des personnes physiques ou morales (art. 17c LApEl) sont concernées, la législation sur la protection des données s'applique et la gestion des données doit s'effectuer conformément aux directives correspondantes dans la mesure où ces données proviennent de systèmes de mesure, de commande et de réglage intelligents. À ce sujet, cf. aussi section 5.7 «Gestion des données des personnes morales».

7.6 Besoins de protection des données

(1) Pour définir les besoins de protection des données existantes, les données pertinentes pour l'entreprise peuvent être collectées sur la base d'un modèle de données ainsi que d'une vue d'ensemble des applications utilisées.

[7] Cf. liste du Préposé fédéral à la protection des données et à la transparence (PFPDT) «Liste des États ayant une législation assurant un niveau de protection adéquat (art. 6, al. 1 LPD)», https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2020/staatenliste.pdf.download.pdf/20200908_Staatenliste_f.pdf

(2) **Modèle de données**

Pour les EAE qui opèrent surtout en tant qu'exploitantes du réseau, un modèle de données simplifié similaire à un catalogue de données peut être utilisé. Celui-ci comprend les données nécessaires pour exécuter le mandat d'approvisionnement pour ses clients et documenter l'exploitation du réseau de distribution:

- les données clients (les clients d'une EAE étant majoritairement des personnes physiques);
- les données pour la documentation des installations propres et les contrats des EAE avec des tiers.
- Des exemples sont donnés au chapitre 9 «Annexe Conformité à la politique des données – modèles de données et applications».

(3) La protection des données s'étend aussi bien aux données personnelles qu'aux données non personnelles:

- Les données personnelles doivent être protégées de façon adéquate en matière de confidentialité et d'intégrité conformément à la Loi fédérale sur la protection des données. Conformément à l'art. 17c LApEl, les données de personnes morales ont aussi ces besoins de protection.
- Les données pour l'exploitation du réseau sont notamment nécessaires pour garantir la sécurité d'approvisionnement. Leur intégrité et leur disponibilité revêtent une importance particulière dans ce cadre.
- Des exemples sont disponibles au chapitre 9 «Annexe Conformité à la politique des données – modèles de données et applications».

(4) **Définition des besoins de protection**

Un exemple de paysage des applications d'une EAE est décrit au chapitre 9 «Annexe Conformité à la politique des données – modèles de données et applications». Les besoins de protection de certaines applications en matière de confidentialité, d'intégrité et de disponibilité sont déduits sur la base des données à traiter et des processus à réaliser. Si plusieurs systèmes sont impliqués dans un processus, les exigences minimales que le système doit respecter sont définies par rapport aux besoins de protection les plus élevés, dans la mesure où il n'est pas possible de réaliser de délimitation systémique.

Applications	Confidentialité	Intégrité	Disponibilité
Système de décompte	Élevée	Élevée	Normale
Relevé des compteurs mobile	Normale	Normale	Normale
Système de relevé des données de mesure (HES, GDM, RCD, smart metering)	Élevée	Élevée	Normale
GDE	Élevée	Élevée	Normale
Télécommande centralisée / gestion de la charge	Normale	Élevée	Élevée
Système SCADA	Normale	Élevée	Élevée
Documentation de l'installation / ensemble de fichiers	Normale	Élevée	Normale

Tableau 4 Exemple des besoins de protection de différentes applications

(5) **Garantie des besoins de protection et des responsabilités**

Pour les systèmes présentant des exigences accrues en matière de besoins de protection, des mesures spécifiques doivent être mises en œuvre afin de réduire les risques. Il est essentiel que les exigences telles que les droits d'accès, la protection des données et le décryptage soient remplies de façon adéquate et en fonction de l'état actuel de la technique.

(6) La responsabilité de la gestion des risques doit être réglée dans toutes les EAE. Dans une EAE, selon la taille de l'entreprise, plusieurs tâches et rôles selon la section 8.2 «Rôles et fonctions» peuvent être assumés par une même personne ou par des tiers. La responsabilité globale de la gestion des risques incombe dans tous les cas à la direction (l'organe dirigeant) de l'EAE.

8. Recommandations de mise en œuvre en matière de gouvernance des données

(1) La gouvernance des données définit des mécanismes et des réglementations pour fixer, mettre en œuvre, entretenir et développer durablement la politique des données. Les tâches, rôles, comités et processus de gouvernance nécessaires sont en outre définis.

(2) Les structures et mesures organisationnelles citées sont des recommandations visant à garantir une mise en œuvre durable de la politique des données au sein de l'entreprise.

8.1 Tâches de la gouvernance des données

(1) Les entreprises sont responsables de la mise en œuvre d'une politique des données adaptée à leurs besoins et de son actualisation. Elles prennent en compte les tâches décrites ci-après. La législation sur la protection des données part alors d'une vision orientée sur les processus.

(2) **Gestion stratégique des données**
Définition et mise en œuvre des prescriptions, directives et politiques interentreprises ainsi que des objectifs contraignants pour la protection et la sécurité des données (confidentialité, intégrité et disponibilité) et pour les tâches opérationnelles de la gestion des données, notamment la gestion de la qualité des données et le reporting des données.

(3) **Inventaire des données**
Pour remplir les exigences de protection et de sécurité des données, un inventaire global (état actuel) de ces dernières est établi et entretenu. Cf. à ce sujet section 5.5 «Traitement des données».

(4) **Gestion de la qualité des données**
On entend par «gestion de la qualité des données» l'ensemble des mesures organisationnelles, techniques et opérationnelles visant à garantir la qualité des données requise du point de vue régulatoire et entrepreneurial. Des processus, grandeurs de mesure et instruments adéquats ainsi qu'une organisation adaptée sont alors utilisés.

(5) **Reporting des données**
Le reporting des données recouvre la création et l'envoi des rapports de données requis du point de vue régulatoire ainsi que la fourniture de données aux destinataires concernés. Les entreprises sont

aussi responsables de la fourniture et du reporting des données dans une qualité adéquate à l'attention des personnes autorisées à utiliser les données, des autorités et des régulateurs. Cette tâche comprend également l'éventuelle obligation de renseigner les autorités et les autres personnes habilitées.

8.2 Rôles et fonctions

(1) En fonction de la forme et de la taille de l'organisation, une même personne peut assumer plusieurs rôles ou ceux-ci sont exécutés par des tiers, la responsabilité restant auprès de l'EAE. Dans les petites entreprises, la direction peut remplir certaines de ces fonctions. Dans les grandes entreprises, ces rôles peuvent être attribués à différentes personnes. Une séparation adéquate des pouvoirs doit toujours être garantie.

(2) Il est recommandé d'introduire les rôles suivants pour accomplir les tâches liées à l'utilisation des données, à la conformité à la politique des données et à la gouvernance des données:

Abréviation	Désignation des rôles et des fonctions	Description des tâches
DPC	Data Protection Consultant / conseiller à la protection des données selon art. 10 LPD	Compétent et responsable pour former et conseiller l'EAE (responsable du traitement) ainsi que pour concourir à l'application des prescriptions relatives à la protection des données et des analyses d'impact relatives à la protection des données personnelles. Autres tâches possibles: – Création et mise à jour du registre des activités de traitement – Établissement et développement de l'organisation de la protection des données au sein de l'entreprise – Rédaction d'une directive d'entreprise pour la protection des données – Examen des produits et services de l'entreprise au regard de la protection des données – Conclusion d'accords de sous-traitance (mandats de traitement de données avec les prestataires externes) – Vérification de la conformité juridique des activités de surveillance – Rédaction d'une directive pour l'utilisation des e-mails et d'Internet au sein de l'entreprise – Rédaction d'autres directives pour la gestion des données personnelles au sein de l'entreprise – Garantie de la protection des données organisationnelles et techniques (MTO) – Réponse aux demandes de renseignements des personnes concernées ou des autorités de surveillance en ce qui concerne le traitement/stockage des données personnelles – Obligations d'annonce selon art. 24 LPD
CISO	Chief Information Security Officer / chef de la sécurité des informations	Compétent pour la sécurité des informations d'une organisation. Tâches possibles:

Abré-viation	Désignation des rôles et des fonctions	Description des tâches
		– Surveillance de la mise en œuvre des recommandations résultant des rapports de révision – Conseil de domaines spécifiques pour des projets de digitalisation et contribution à la conception de solutions modernes dans le cadre de projets – Surveillance de la situation en matière de sécurité et évaluation des analyses de risque – Définition des normes de sécurité des données et vérification de leur respect – Soutien des domaines opérationnels dans leurs tâches et surveillance systématique des activités menées – Obligations d'annonce en cas d'incidents critiques à la cybersécurité: selon NCSC/DDPS (état 01.22, encore en consultation)
CSO	Chief Security Officer / chef de la sécurité	Compétent et responsable pour toutes les questions relatives à la sécurité physique (bâtiments, clés, accès...). Tâches possibles: – Mise en œuvre des directives de sécurité dans l'activité quotidienne – Garantie de l'introduction de contrôles techniques, physiques et procéduraux – Rédaction de directives, mise à disposition de ressources, soutien et vérification de la protection physique adéquate des informations au sein du domaine de compétence – Information sur les recommandations faites par les employés/fournisseurs – Information sur les infractions avérées ou supposées aux directives (incidents de sécurité) – Vérification du respect de la politique de sécurité et réalisation d'audits internes occasionnels
CO	Compliance Officer	– Identification et évaluation des risques en cas de non-respect des directives par l'entreprise – Évaluation des risques de sanctions judiciaires, administratives ou disciplinaires, de pertes financières considérables ou d'atteinte importante à la réputation découlant du non-respect de dispositions (législatives ou régulatoires) spécifiques, de normes professionnelles ou éthiques ou d'instructions de l'organe exécutif – Fonction d'information, de formation et de conseil pour les collaborateurs de tous niveaux hiérarchiques

Tableau 5 Vue d'ensemble des rôles et fonctions pertinents pour la politique des données

(3) La responsabilité globale de la définition, de la mise en œuvre, de l'entretien ainsi que du perfectionnement durable des réglementations relevant de la politique des données incombe à la direction de l'entreprise. Il est recommandé de former régulièrement les collaborateurs de façon appropriée.

(4) L'entreprise est tenue, en cas d'incident, de prouver que les précautions nécessaires avaient été prises.

(5) La figure suivante illustre l'interaction entre la sécurité des informations et la protection des données:

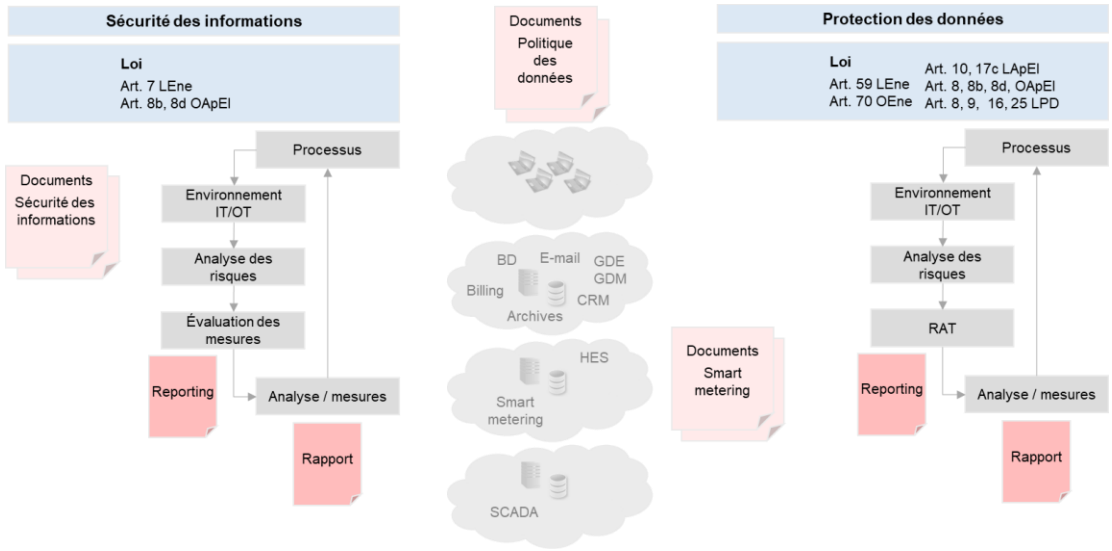


Figure 8 Interaction entre la sécurité des informations et la protection des données

- Le CISO analyse les exigences en matière de sécurité des informations et définit des mesures. Pour maintenir le niveau de sécurité, fluctuant, un processus de garantie de la qualité est défini.
- Le DPC analyse les flux d'informations au sein de l'entreprise, effectue une analyse des risques et définit les principes pour l'accès et l'utilisation des données. Il veille à ce que le tableau RAT soit rempli.
- Un système approprié de gestion de la protection des données garantit notamment l'amélioration continue, une organisation adéquate et un reporting régulier à la direction de l'entreprise.

8.3 Registre des activités de traitement

(1) Le registre des activités de traitement (RAT), décrit à l'annexe du même nom, peut servir de base pour l'établissement du registre conformément à la section 5.5 «Traitement des données».

(2) Le RAT donne des renseignements sur tous les aspects essentiels du traitement des données (au sens d'une exigence minimale) pour toutes les catégories de données de l'entreprise listées: de la collecte à la suppression, en passant par le traitement et la transmission.

(3) Les informations contenues dans le RAT sont en outre utiles pour traiter le thème de l'IT et de la cybersécurité.

(4) Le RAT est un outil crucial pour la mise en œuvre de la politique des données. Il recouvre les aspects commerciaux et informatiques et suppose une approche, un traitement et une mise à jour intersectoriels.

(5) Le RAT sert de point de départ pour la détermination et la mise en œuvre de mesures de sécurité techniques et organisationnelles. Il est aussi possible d'utiliser, à titre de soutien, les normes telles

que la suite ISO/IEC-27000 ou d'autres réglementations de «best practice». Voir aussi la section 6.2.1 du rapport de l'AES sur la politique des données dans le secteur énergétique, avec les meilleures pratiques et normes disponibles à ce jour, pour la création, la mise en œuvre et l'entretien de la gestion de la sécurité des informations (GSI) ou d'un système de management de la protection de la vie privée (Privacy Information Management System, PIMS).

(6) La structure recommandée pour le RAT est consultable au chapitre 11 «Annexe Gouvernance des données – registre des activités de traitement».

9. Annexe Conformité à la politique des données – modèles de données et applications

Modèle de données

(1) Les données suivantes des clients d'une EAE font l'objet d'une gestion et d'un traitement (liste non exhaustive):

- Données client (p. ex. dans le rôle du partenaire contractuel, du destinataire de la facture, du propriétaire)
  - Nom, prénom, nom de l'entreprise
  - Adresse, adresse de livraison
  - Bâtiment
- Données contractuelles
  - Contrats de fourniture d'électricité, contrats de raccordement au réseau et contrats d'utilisation du réseau avec durée de validité.
  - Groupes de consommation / types de consommation
  - Produit, éléments de prix, périodes de facturation
  - Adresse de facturation
  - Éventuellement informations relatives à l'encaissement
  - Éventuellement données prévisionnelles
- Données de mesure
  - Données de décompte / données de consommation (puissance active, énergie réactive, puissance)
  - Données de la courbe de charge si disponibles (avec une granularité maximale de 15 minutes)
  - Éventuellement valeurs locales de courant ou de tension
- Données d'installation
  - Puissance de raccordement, valeurs de protection, mise à zéro, accès...
  - Indications de grands consommateurs (chaudière, pompes à chaleur, dispositif de stockage, machine à laver…)
  - Indications d'installations de production (technologie, puissance...)
  - Compteur, récepteur de télécommande avec commandes utilisées

(2) La documentation des installations d'une EAE et les contrats qu'elle a passés avec des tiers comprennent les informations suivantes (liste non exhaustive):

- Documentation des installations (données d'actifs)
- Données SIG
- Données de mesure issues du réseau (p. ex. qualité du réseau)
- Données contractuelles avec les fournisseurs et prestataires
- Éventuellement données SCADA

(3) Les données personnelles doivent être protégées de façon adéquate en matière de confidentialité et d'intégrité conformément à la Loi fédérale sur la protection des données. Sont considérées comme des données personnelles (liste non exhaustive):

- Données client

    - Nom, prénom
    - Adresse
- Données contractuelles
    - Groupes de consommation / types de consommation
    - Informations relatives à l'encaissement
    - Données prévisionnelles
- Données de mesure
    - Données de la courbe de charge (avec une granularité maximale de 15 minutes)
- Données d'installation
    - Récepteur de télécommande avec commandes utilisées
    - Données générales de commande

(4) Les données pour l'exploitation du réseau sont notamment nécessaires pour garantir la sécurité d'approvisionnement. Leur intégrité et leur disponibilité sont essentielles. Les données à protéger sont (liste non exhaustive):

- Données de mesure chez le client
    - Données de la courbe de charge (avec une granularité maximale de 15 minutes)
    - Valeurs de courant ou de tension locales
- Données d'installation chez le client
    - Indications de grands consommateurs (chaudière, pompes à chaleur, dispositif de stockage, machine à laver…)
    - Indications d'installations de production (technologie, puissance...)
- Données du gestionnaire de réseau
    - Documentation des installations (données d'actifs)
    - Données de mesure issues du réseau (p. ex. qualité du réseau)
    - Données SCADA

10. Annexe Conformité à la politique des données – données issues de l'exploitation du réseau et de l'approvisionnement de base

(1) **Description du paysage simplifié des applications d'une EAE**

Les données liées à des clients sont en général saisies et mises à jour dans un système de décompte. Les données de décompte sont souvent relevées par un collaborateur sur place à l'aide d'un système de relevé des compteurs et transmises au système de décompte.
Le relevé des compteurs à distance (aussi bien traditionnel que via un système de smart metering / SMI) est fréquemment sous-traité à un prestataire. Le même principe s'applique au système de gestion des données énergétiques. Ces systèmes sont généralement couplés par le biais d'interfaces fichiers.
Pour la gestion de la charge, une installation de télécommande centralisée fournie par l'EAE et exploitée avec le soutien du fabricant est aujourd'hui utilisée dans de nombreux cas. Dans le cadre du déploiement des smart meters, celle-ci est partiellement remplacée par une gestion de la charge basée sur le smart metering.
La documentation des installations s'effectue dans un système ad hoc, qui provient en partie du même fabricant que le système de décompte. La documentation complémentaire est en général archivée sur la base des fichiers ou n'existe qu'en version papier.

(2) Vous trouverez ci-après un exemple de vue d'ensemble des exigences en matière de protection des données qui doivent être remplies au cours des différentes étapes du traitement des données.

Exigences en matière de protection des données	Étape du processus	Types de données	kWh / DC	HES	GDM	Systèmes de réglage	GDE	Partenaires de marché	Profilage	Billing	Portail
			Données des courbes de charge	Données des courbes de charge	Données des courbes de charge	N° de compteur	Données des courbes de charge	Données des courbes de charge	Données des courbes de charge	États du compteur	États du com
			États du compteur	États du compteur	États du compteur	N° de commutateur de charge	Metering Code	Metering Code	Metering Code	Avances du compteur	Données des courbes de c
			N° de compteur	N° de compteur	N° de compteur	Données de commande				Sommes des courbes de charge	Metering Coc
			Type de compteur	Type de compteur	Type de compteur					Metering Code	Données d'adresse
				Metering Code	Metering Code					Données d'adresse	Données de facturation
					Données d'adresse					Pas de données CCI	
	Collecte des données		Relevé des données	Plausibilisation Validation Décompte Attribution avec un tableau de mappage	Pilotage du réseau Condition préalable: connexion via les groupes	Gestion du bilan d'ajustement Décompte		Profilage	Facturation	Visualisation	
Données pseudonymisées (via n° de compteur)			Données pseudonymisées (via n° de compteur)	Données non pseudonymisées	Données anonymisées	Données pseudonymisées (via MC)		Données pseudonymisées (via MC)	Données non pseudonymisées	Données non pseudonymis	
Données personnelles			Données personnelles	Données personnelles	Données non personnelles	Données personnelles		Données personnelles	Données personnelles	Données personnelles	
						Pas d'accès au tableau de mappage		Pas d'accès au tableau de mappage	Accord préalable du client	Pas de courbes de charge dans le système de billing	

Figure 9 Exemple de vue d'ensemble des exigences en matière de protection des données issues de l'exploitation du réseau et de l'approvisionnement de base

11. Annexe Gouvernance des données – registre des activités de traitement

(1) Il est possible d'établir un modèle de registre des activités de traitement (RAT) de la manière suivante. Il correspond aux exigences minimales conformément à l'art. 12 LPD et comprend également des données dans le cadre de la sous-traitance de données. Les parties 1/3 à 3/3 forment un tableau cohérent.

Registre des activités de traitement du responsable du traitement

Nom et adresse du responsable	Représentant légal (= direction)	Représentant au sein de l'UE (art. 27, al. 1, en relation avec l'art. 3, al. 2 RGDP)		Nom et coordonnées (adresse, e-mail et évent. autres) de la personne chargée de la protection des données

N°	Désignation de l'activité de traitement	Domaine spécialisé responsable	Contient des données personnelles UE	Nom du responsable du traitement	Lieu du traitement	Finalité du traitement

Date:
Signature:

Tableau 6 Modèle de registre des activités de traitement – partie 1/3

Autorités de surveillance compétentes	Réglementations relatives à la sécurité des données	Réglementations relatives à la suppression des données
PFPDT…	Instruction relative à la sécurité des informations…	

Catégorie de personnes concernées	Catégorie de données personnelles	Catégories de destinataires

Tableau 7 Modèle de registre des activités de traitement – partie 2/3

Faits relatifs aux transferts à des pays tiers	évent. Joint Controller
Data Transfer Agreement…	

Transferts de données dans des pays tiers ou des organisations internationales		Délais prévus pour la suppression des diverses catégories de données	Description générale des mesures techniques et organisationnelles (MTO)
Transfert	Noms des pays tiers		

Tableau 8 Modèle de registre des activités de traitement – partie 3/3

(2) Ci-après se trouvent des explications et indications relatives aux catégories utilisées dans le RAT:

Détails → Catégorie ↓	**Formes possibles**	**Thématiques possibles**	**Remarques**
Représentant à l'UE			Pour le cas où des données sont collectées et/ou traitées dans la zone de l'UE.

Détails → Catégorie ↓	**Formes possibles**	**Thématiques possibles**	**Remarques**
Désignation de l'activité de traitement	Metering, GRH, marketing	Quelles données font l'objet d'un traitement? Où les données sont-elles traitées? Dans quel objectif les données sont-elles traitées?	Des catégorisations génériques sont possibles, mais on ne peut procéder à aucune «forfaitisation».
Catégories de traitements cf. chapitre 3, paragraphe (3)			
Entité juridique ou domaine spécialisé responsable			
Comprend des données personnelles UE	Oui / Non		Le cas échéant, pertinence pour la décision d'applicabilité du RGPD-UE
Nom du responsable	Nom, prénom		
Lieu du traitement	Territoire et prestataire	Où se trouvent p. ex. les serveurs? Des services basés sur le cloud sont-ils utilisés?	Pertinence pour la décision d'applicabilité de la LPD ou du RGPD-UE
Objectifs des traitements	Production, gestion du personnel…	Motif du traitement des données	Important car ces derniers définissent l'affectation
Catégorie de personnes concernées	Collaborateurs, clients, soumissionnaires, personnes intéressées...		
Catégorie de données personnelles	Données personnelles, données personnelles particulièrement sensibles, profilage	Quels contenus sont traités et comment?	Déduction de la protection nécessaire ou de la pertinence de la protection (dans le cas du profilage)
Catégories de destinataires (public, interne, externe)	Tiers, autorités...	À qui sont transmises les données?	P. ex. information dans les CGV et les contrats
Transferts de données dans des pays tiers ou à des organisations internationales / provenance	Allemagne...	Des données sont-elles transmises à l'étranger et, le cas échéant, dans quel pays et à qui?	Contrôle de l'adéquation conformément à la liste PFPDT
Délais prévus pour la suppression des diverses catégories de données	Délais possibles: 12 mois 5 ans 10 ans Délais spécifiques	Combien de temps certaines données doivent-elles être conservées avant d'être supprimées?	La suppression peut être exigée ou doit avoir lieu en vertu de la loi. Cela nécessite des adaptations au niveau informatique.

Description générale des mesures techniques et organisationnelles (MTO)
Les MTO constituent une partie essentielle de la documentation relative à la protection des données et sont cruciales pour le RAT, la sous-traitance et les contrats correspondants, ainsi que pour les obligations d'information et de transparence. Elles peuvent notamment comprendre les domaines suivants: 1. **Pseudonymisation** Procédure consistant à remplacer les données personnelles par des suites de chiffres p. ex., de sorte qu'elles ne puissent plus être attribuées à une personne. Cf. exemple du point de mesure au chapitre 3 «Définitions». 2. **Cryptage** Protection des données contre l'accès non autorisé, p. ex. pendant leur transfert. 3. **Garantie de la confidentialité** Réglementation de l'accès visant à garantir que seules les personnes autorisées ont accès aux locaux, serveurs, etc. 4. **Garantie de l'intégrité** Procédure visant à garantir que les données traitées sont correctes, non falsifiées et authentiques. Gestion des modifications, suppressions, etc. 5. **Garantie de la disponibilité** Mesures garantissant la disponibilité des données, systèmes, etc., en cas de panne d'électricité p. ex. 6. **Garantie de la résistance des systèmes** Ensemble des mesures visant à garantir la protection adéquate des systèmes contre les incidents, les intrus ou autres. 7. **Procédure de rétablissement de la disponibilité des données personnelles après un incident physique ou technique** Mesures et techniques garantissant que les données, systèmes, etc. sont de nouveau disponibles en cas de dommage (y c. contenu adéquat). 8. **Procédure de contrôle, d'appréciation et d'évaluation réguliers de l'efficacité des mesures techniques et organisationnelles** Marche à suivre pour examiner, adapter, renouveler, etc. régulièrement les mesures prises. 9. **Documentation écrite des autres mesures** Formation de collaborateurs, réglementations et instructions, certifications, etc.

Tableau 9 Catégories, explications et indications relatives au registre des activités de traitement

(3) Cette version de base peut être complétée par d'autres tableaux au sens d'un référentiel TIC – par exemple par des tableaux représentant des systèmes, des aspects de la sécurité, des autorisations d'accès, des autorisations de renseignement, etc.

12. Annexe FAQ RGPD

Ces questions & réponses (FAQ) représentent des principes qui ne doivent cependant pas être considérés comme des renseignements juridiques contraignants. Dans certains cas individuels ou certaines constellations, des divergences notables sont possibles.

Question 1: Le RGPD est-il applicable lorsque des collaborateurs en télétravail à l'étranger traitent des données de l'EAE, peu importe que les données soient traitées sur un serveur de l'EAE, dans un centre informatique en Suisse ou dans l'UE, ou localement (sur le terminal)?

Réponse 1: En principe, l'accès à des données et leur consultation sont aussi considérés comme un traitement de données; d'un point de vue strictement juridique, une application du RGPD en résulte par conséquent pour ce processus.

Question 2: Le RGPD est-il applicable lorsque j'utilise un prestataire de services établi dans l'UE pour des prestations de support informatique, p. ex., et que l'accès aux données se fait depuis l'UE?

Réponse 2: En principe, l'accès à des données et leur consultation sont aussi considérés comme un traitement de données; d'un point de vue strictement juridique, une application du RGPD en résulte par conséquent pour ce processus.

Question 3: Le RGPD est-il applicable lorsque des données de l'EAE sont stockées dans un centre informatique prestataire dans l'UE?

Réponse 3: En principe, le stockage de données est aussi considéré comme un traitement de données; d'un point de vue strictement juridique, une application du RGPD en résulte par conséquent pour ce processus.

Question 4: Le RGPD est-il applicable lorsque je livre de l'électricité à des clients finaux sur territoire suisse (p. ex. dans un appartement ou une maison de vacances) et que le client est originaire de l'UE?

Réponse 4: Non, les données proviennent de personnes venant de Suisse ou se trouvant dans une relation contractuelle relevant du droit suisse.

Question 5: Le RGPD est-il applicable lorsque des personnes venant de l'UE utilisent ma boutique en ligne ou mon site Internet en Suisse?

Réponse 5: En principe, non. Des divergences sont possibles, en particulier lorsqu'elles dépendent des facteurs suivants, p. ex.: si une terminaison de nom de domaine autre que .ch est utilisée, ou si des langues qui ne sont pas des langues nationales sont utilisées (y c. l'anglais), les prix peuvent aussi être convertis en € ou sont affichés directement en €.

Question 6: Le RGPD est-il applicable lorsqu'une EAE collecte activement des données de personnes venant de l'UE (p. ex. indexation de site/*website crawling*) ou lance un concours dont le groupe cible inclut des personnes de l'UE?

Réponse 6: Oui, dans ce cas, des données de personnes venant de l'UE sont traitées ou collectées de manière ciblée. La finalité principale n'est pas de remplir une obligation contractuelle, mais de prélever de manière ciblée des données («principe du lieu du marché» ou *Marktortprinzip*). Le lieu du traitement est ainsi sans importance.

Question 7: Le RGPD est-il applicable lorsque certaines personnes figurant dans mon envoi de newsletter (numérique ou physique) ont leur domicile dans l'UE?

Réponse 7: En principe, non. On part de l'hypothèse que la personne concernée a enregistré elle-même ses données et que l'information et la transparence existaient lors de la collecte des données. De plus, avec une newsletter, l'activité et le contenu ne visent PAS en premier lieu des personnes ou d'autres relations avec l'UE, et cela représente donc une quantité minime des clients de la newsletter.

Question 8: Lorsqu'un certain traitement des données se fait sous le régime du RGPD, tous les autres traitements de données doivent-ils aussi se faire conformément au RGPD?

Réponse 8: Non. Le traitement spécifique des données doit se faire en respectant le RGPD, ce qui n'entraîne cependant pas que tous les processus de l'ensemble de l'EAE y soient soumis.

Question 9: Lorsqu'une EAE respecte soit le RGPD, soit la LPD suisse, l'autre législation est-elle automatiquement couverte aussi?

Réponse 9: Non. Bien que les deux législations sur la protection des données soient très semblables, elles présentent aussi des différences dans quelques domaines.

Question 10: L'EAE est-elle soumise au RGPD lorsque des marchandises et/ou des prestations de services sont acquises depuis l'UE?

Réponse 10: Non. En cas d'acquisition de marchandises et de prestations de services, ce n'est généralement pas le traitement des données qui est central, sauf si les données et informations constituent elles-mêmes les marchandises et les prestations de services (p. ex. achat de données d'adresses de personnes venant de l'UE). L'achat d'objets physiques (p. ex. papier à photocopies) dans l'UE n'est donc pas soumis au RGPD.

13. Guide concernant les principaux éléments de mise en œuvre de la politique des données

Les principaux aspects et propositions pour la mise en œuvre de la politique des données sont listés succintement ci-après:

(1) Préparatifs généraux

- ✓ Planification des ressources pour la mise en œuvre
  - La mise en œuvre de la politique des données à l'échelle de l'entreprise est un projet qui dure plusieurs années.
  - Les ressources correspondantes doivent être disponibles.
- ✓ Changement de culture
  - Il est nécessaire d'avoir conscience de l'importance de ce thème dans l'entreprise.
  - C'est l'affaire des chefs: le processus de changement doit être initié et porté activement par la direction de l'entreprise.
  - La responsabilité de la mise en œuvre ne peut pas être déléguée aux collaboratrices et collaborateurs.
- ✓ Bien se rendre compte de la différence entre protection des données et sécurité des données (sections 7.1 et 7.2)
  - Avec la digitalisation, protection des données et sécurité des données deviennent toujours plus importantes et ne peuvent pas être considérées séparément.

(2) Fondements juridiques (chapitre 4)

- ✓ Garantie du respect des prescriptions de la LApEl
  - Séparation des activités au niveau de l'information selon art. 10, al. 2 LApEl (section 6.1)
  - Mesures pour délimiter l'exploitation du réseau des autres entités organisationnelles (en particulier la vente d'énergie) implémentées?
  - Cloisonnement de l'accès à l'information pour les collaboratrices et collaborateurs au sein du GRD garanti?
- ✓ Art. 8d OApEl
  - Profils
  - Intervalle de mesure de 15 minutes
  - Pseudonymisation
  - Consentement
  - Dispositions cantonales (clarifier si des dispositions cantonales donnent des prescriptions plus strictes que celles de la Confédération)
- ✓ L'entreprise est-elle soumise à la LPD et/ou au RGPD?
  - Une aide figure dans l'Annexe FAQ RGPD du document Politique des données.

(3) Mise en œuvre de l'utilisation des données et de la conformité à la politique des données

- ✓ Effectuer une analyse de la protection des données (section 7.1)
  - Principe du besoin de connaître (*need to know*) (chapitre 3, paragraphe (6))
  - Établir un registre des activités de traitement (section 8.3 et Annexe Gouvernance des données – registre des activités de traitement)
    - Inclure les modèles de processus s'ils existent (voir rapport de l'AES sur la politique des données)
    - Cycle de vie des données (chapitre 4)
    - Que les données se présentent sous forme numérique ou physique n'a pas d'importance

- Identifier les données personnelles
- Identifier les autres données critiques de l'entreprise (soumises au secret professionnel, données SIG, données SCADA,…; section 7.5)

✓ Sécurité des données: effectuer une analyse des risques (section 7.2)
- Confidentialité: quelles données ai-je le droit de transmettre vers l'extérieur?
- Intégrité: puis-je garantir que les données sont correctes?
- Disponibilité: les données sont-elles disponibles lorsque j'en ai besoin?
- Authentification: est-il garanti que l'identité d'un utilisateur peut être prouvée par rapport au système?
- Autorisation: qui, dans l'entreprise, a le droit de voir quelles données?
- Suivi: est-il garanti que les modifications de données restent compréhensibles?

✓ Implication de tiers (section 6.4)
- Externalisation de prestataires de services
- Utilisation de services Cloud (p. ex. Office 365)
- Une externalisation à des tiers ne dégage pas l'EAE de la responsabilité

✓ Définir les besoins de protection des données (section 7.6)
- sur la base du registre des activités de traitement
- Données pour la documentation des installations et des contrats dans l'EAE

✓ Mettre en œuvre les mesures issues des analyses de protection des données et de risque (annexe, description des MTO)
- Introduire des mesures techniques et organisationnelles pour réduire les risques
- La mise en œuvre des MTO prendra plusieurs années

✓ Consentement des clients si un traitement des données plus étendu est effectué, p. ex. (sections 6.2, 6.3):
- Données avec une granularité maximale de 15 minutes
- Lecture des données des appareils sur le terrain plus fréquente que 1x par jour
- Lecture des données en temps réel
- Visualisation des données relevées toutes les 15 minutes dans un portail clients
- Transmission des données à des tiers

✓ Suppression des données (section 7.3)
- Droit à l'oubli
- Après 12 mois lorsqu'elles ne sont pas utilisées pour le décompte
- Après 5 ans lorsqu'elles sont utilisées pour le décompte
- Après 10 ans pour la facture effective aux clients
- Pour poursuivre l'utilisation, demander l'accord des clients
- Quelles données doivent être anonymisées?
- Archivage: garantir que les données soient aussi supprimées dans les archives/la sauvegarde

(4) Mise en œuvre de la gouvernance des données (chapitre 8)

✓ Rôles / fonctions (section 8.2)
- La responsabilité globale incombe à la direction de l'entreprise.
- Guide Conseiller à la protection des données (DPC, Data Protection Consultant)
  - Vérification régulière et systématique des réglementations et lois importantes pour le marché de l'électricité, en particulier LPD, RGPD, délais transitoires, gestion des données de personnes morales
- Selon la LPD, les collaborateurs sont personnellement responsables en cas de violation de la protection des données
- Chef de la sécurité des informations (CISO; Chief Information Security Officer)
- Chef de la sécurité (CSO, Chief Security Officer)

- Compliance Officer (CO)
- Les rôles peuvent être attribués à des collaborateurs existants; il est également possible d'attribuer plusieurs rôles à une même personne ou d'externaliser les rôles à des tiers. Restriction: un rôle ne peut pas se contrôler lui-même.

✓ Formation périodique de tous les collaborateurs (conscience des collaborateurs)
✓ Définir un interlocuteur pour les annonces d'incidents liés à la protection et à la sécurité des données

14. Glossaire

Abréviation	Description
AAA	Authentication / Authorization / Accounting
AES	Association des entreprises électriques suisses
BD	Base de données
CEI	Commission électrotechnique internationale
CGV	Conditions générales de vente
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
CO	Compliance Officer
CRM	Customer Relationship Management (gestion de la relation client)
CSO	Chief Security Officer
DMI	Dispositif de mesure intelligent
DPC (auparavant: DPO)	Data Protection Consultant (conseiller à la protection des données selon art. 10 LPD) (appelé auparavant Data Protection Officer)
EAE	Entreprise d'approvisionnement en énergie
ERP	Enterprise Resource Planning (progiciel de gestion intégrée)
GDE	Gestion des données énergétiques
GDM	Gestion des données de mesure
GRD	Gestionnaire de réseau de distribution
GT	Groupe de travail
HES	Head End System (système de tête de réseau)
ISO	Organisation internationale de normalisation
IT	Information Technology (technologies de l'information, informatique)
LApEl	Loi sur l'approvisionnement en électricité
LEne	Loi sur l'énergie
LPD	Loi fédérale sur la protection des données
MTO	Mesures techniques et organisationnelles
OApEl	Ordonnance sur l'approvisionnement en électricité
OEne	Ordonnance sur l'énergie
OLEl	Ordonnance sur les lignes électriques
Olico	Ordonnance concernant la tenue et la conservation des livres de compte
OLPD	Ordonnance relative à Loi fédérale sur la protection des données
OT	Operational Technology
PFPDT	Préposé fédéral à la protection des données et à la transparence
RAT	Registre des activités de traitement
RCD	Relevé des compteurs à distance
RGPD-UE	Règlement général de l'Union européenne sur la protection des données (ci-après: RGPD)

Abréviation	Description
SCADA	Supervisory control and data acquisition
SIG	Système d'information géographique
SMI	Système de mesure intelligent. Désigne toute la chaîne de mesure à partir du DMI (smart meter) jusqu'au HES (Head End System, système de tête de réseau) via le concentrateur de données ou la passerelle (Gateway), quelle que soit la technologie de transfert.
TIC	Technologies de l'information et de la communication
UE	Union européenne