



Recommandation de la branche

Politique des données dans la branche énergétique

Cadre de gestion globale des données dans la branche énergétique

DPE – CH, édition juillet 2019

Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Téléphone +41 62 825 25 25, fax +41 62 825 25 26, info@electricite.ch, www.electricite.ch



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	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	SWiBi	Membre du groupe de travail

Responsabilité du groupe de travail

Le groupe de travail Data Policy de l'AES est désigné responsable de la tenue à jour et de l'actualisation du document.



Chronologie

Date	"Brève description"
Juin 2018	Planification des travaux pour la recommandation de la branche
Décembre 2018	Pré-approbation de la recommandation de la branche par le groupe de travail Data Policy
Juillet 2019	Approbation 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 02.07.2019.

Imprimé N° 2002/f, édition 2019

Copyright

© Association des entreprises électriques suisses AES

Tous droits réservés. L'utilisation des documents pour un usage professionnel n'est permise qu'avec l'autorisation de l'AES et contre dédommagement. Sauf pour un usage personnel, toute copie, toute distribution ou tout autre usage de ce document sont interdits. Les auteurs déclinent toute responsabilité en cas d'erreur dans ce document et se réservent le droit de le modifier en tout temps sans préavis.

Égalité linguistique des sexes

La forme masculine est utilisée par défaut dans le présent document afin d'en faciliter la lecture. Tous les rôles et toutes les désignations de personnes sont néanmoins susceptibles de se rapporter aussi bien à des femmes qu'à des hommes. Nous vous remercions de votre compréhension.



Table des matières

Avant-propos	6
1. Introduction.....	7
1.1 Généralités	7
1.2 Objectif du document	7
1.3 Intégration de la politique des données dans le paysage documentaire de l'AES	8
2. Domaine d'application.....	10
3. Vue d'ensemble de la mise en œuvre de la politique des données	10
4. Fondements juridiques.....	11
4.1 Vue d'ensemble des réglementations, des lois et des normes ainsi que des limitations	12
4.2 Données personnelles	12
4.3 Données personnelles particulièrement sensibles.....	13
4.4 Données présentant des besoins de protection supérieurs (profilage)	14
4.5 Traitement des données	14
4.6 Gestion des données des personnes morales.....	15
5. Définitions.....	15
6. Recommandations de mise en œuvre en matière d'utilisation des données	17
6.1 Séparation au niveau de l'information.....	17
6.2 Utilisation des données issues de l'exploitation du réseau et de l'approvisionnement de base	18
6.3 Utilisation des données issues de systèmes de mesure intelligents du GRD	19
6.4 Autres secteurs d'activité	20
6.5 Implication de tiers	20
7. Recommandations de mise en œuvre en matière de conformité à la politique des données	21
7.1 Protection des données	21
7.2 Sécurité des données	22
7.3 Traitement des données de mesure conformément à l'OApEI	22
7.4 Gestion approfondie des données personnelles.....	24
7.5 Gestion des données non personnelles.....	25
7.6 Besoins de protection des données.....	25
8. Recommandations de mise en œuvre en matière de gouvernance des données	26
8.1 Tâches de la gouvernance des données	26
8.2 Rôles et fonctions.....	27
8.3 Registre des activités de traitement.....	30
9. Annexe Conformité à la politique des données – modèles de données et applications.....	31
10. Annexe Conformité à la politique des données – données issues de l'exploitation du réseau et de l'approvisionnement de base	34
11. Annexe Gouvernance des données – registre des activités de traitement	35
12. Glossaire	39



Liste des figures

Figure 1	Thèmes-clés de la politique des données	8
Figure 2	La politique des données, cadre pour les documents de l'AES portant sur des thèmes voisins	9
Figure 3	Thèmes abordés dans le cadre de la mise en œuvre de la politique des données	10
Figure 4	Exemple de mise en œuvre de la pseudonymisation avec un tableau de mappage	16
Figure 5	Exemple de mise en œuvre de l'anonymisation	16
Figure 6	Utilisation des données issues de SMI (art. 8d OApEI) en lien avec la séparation au niveau de l'information (art. 10, al. 2, LApEI)	20
Figure 7	Directives relatives à l'obligation de conservation des données personnelles	23
Figure 8	Interaction entre la sécurité des informations et la protection des données	29
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	34

Liste des tableaux

Tableau 1	Vue d'ensemble des documents de l'AES concernés par la politique des données	9
Tableau 2	Vue d'ensemble des réglementations	12
Tableau 3	Catégories de données personnelles particulièrement sensibles	14
Tableau 4	Exemple des besoins de protection de différentes applications	26
Tableau 5	Vue d'ensemble des rôles et fonctions pertinents pour la politique des données	29
Tableau 6	Modèle de registre des activités de traitement – partie 1/3	35
Tableau 7	Modèle de registre des activités de traitement – partie 2/3	35
Tableau 8	Modèle de registre des activités de traitement – partie 3/3	36
Tableau 9	Catégories, explications et indications relatives au registre des activités de traitement	38



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 ouvert 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 (LApEI) et par l'Ordonnance sur l'approvisionnement en électricité (OApEI).

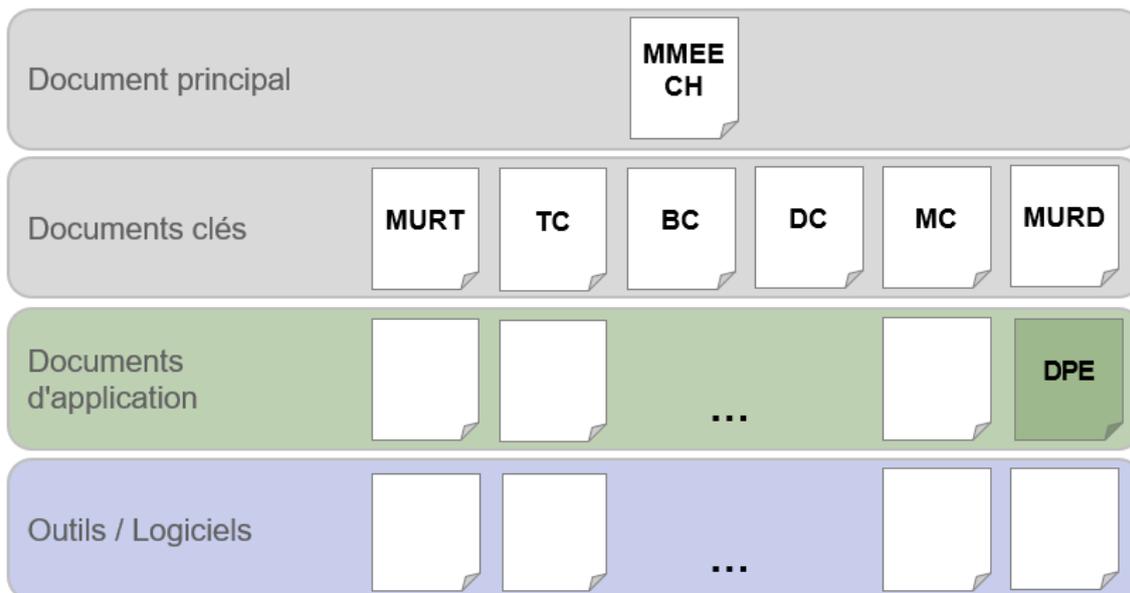
Les documents de la branche sont élaborés par des spécialistes de la branche selon le principe de subsidiarité; ils sont régulièrement mis à jour et complétés. Les dispositions qui ont valeur de directives au sens de l'OApEI sont des normes d'autorégulation.

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 commerciales¹, 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) Les répercussions de la digitalisation ont mené en mai 2018 à l'entrée en vigueur de la nouvelle législation de l'UE, qui a une influence à la fois sur la **législation** suisse **sur la protection des données** et sur les entreprises opérant en Suisse.
- (3) Le 1^{er} janvier 2018, le droit relatif à l'approvisionnement en électricité a fixé les conditions-cadre pour les EAE – notamment 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 (art. 17c LApEI, art. 8d OApEI). Les prescriptions fédérales sur la protection des données s'appliquent dans ce cadre.
- (4) Les directives de **séparation au niveau de l'information**, conformément à l'art. 10, al. 2, LApEI, doivent également être prises en compte.
- (5) Les infractions aux exigences réglementaires 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.
- (6) Le présent document se fonde sur le rapport de l'AES sur la politique des données dans le secteur énergétique², qui expose les bases pour l'élaboration de l'actuelle politique des données après une analyse des conditions-cadre juridiques ainsi que des particularités et évolutions au sein de la branche énergétique.
- (7) Dans le présent document, le terme d'«utilisateur du réseau» désigne le consommateur final et/ou le producteur et/ou le 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

² «Bericht Data Policy in der Energiebranche», consultable en allemand (avec Management Summary en français) sur www.electricite.ch, à la rubrique «Téléchargement», type «Document spécialisé».



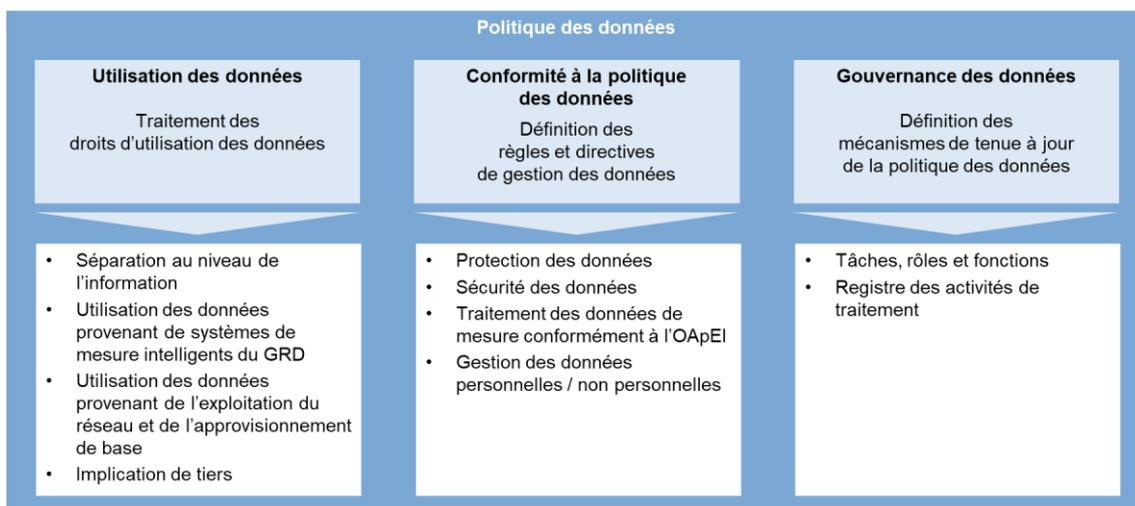


Figure 1 Thèmes-clés de la politique des données

- (2) La présente politique des données sert de guide ou d'outil pour les entreprises liée à la branche énergétique dans l'objectif d'une gestion homogène des données. De manière générale, les grandes EAE disposent d'ores et déjà de concepts de solutions et de ressources qui traitent des thèmes abordés par la recommandation de la branche. La politique des données vise également à fournir un document pratique de gestion des données aux petites et moyennes entreprises. 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 politique des données sert de cadre global pour la gestion des données dans la branche énergétique:
- Elle s'applique à des thèmes fondamentaux dans le domaine des technologies de l'information et de la communication, tels que la continuité des TIC («ICT Continuity») et la sécurité des technologies opérationnelles et de l'information («IT / OT Security»).
 - Dans ce contexte, elle se rapporte aux sujets spécifiques à la branche énergétique, notamment le système de mesure, la communication marché, les systèmes, etc.
- (2) 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.



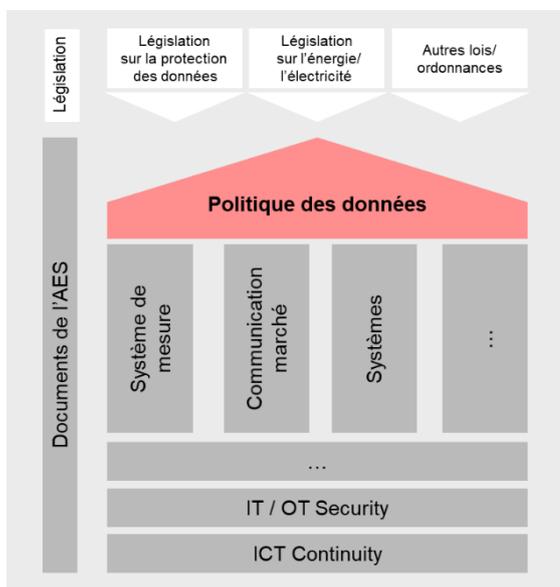


Figure 2 La politique des données, cadre pour les documents de l'AES portant sur des thèmes voisins

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

Thème	Document
Politique des données	<ul style="list-style-type: none"> – Rapport sur la politique des données dans le secteur énergétique – Recommandation de la branche «Politique des données dans la branche énergétique»
Système de mesure	<ul style="list-style-type: none"> – Document-clé «Metering Code Suisse» – Directives pour la sécurité des données des systèmes de mesure intelligents – Manuel «Gestion des données de mesure» – Manuel «Smart Metering CH» – Document thématique «Protection et sécurité des données dans le cadre du smart metering» – Document thématique «Responsabilité dans le domaine de la métrologie»
Communication marché ³	<ul style="list-style-type: none"> – 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» – Manuel «Gestion des données de mesure»
Systèmes	<ul style="list-style-type: none"> – Manuel «Systèmes de commande et de réglage intelligents pour l'exploitation du réseau»
IT / OT Security	<ul style="list-style-type: none"> – Manuel «Protection de base pour les «technologies opérationnelles» (OT) dans l'approvisionnement en électricité»
ICT Continuity	<ul style="list-style-type: none"> – Recommandation de la branche «ICT Continuity»
...	<ul style="list-style-type: none"> – 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

³ Y compris la mise à disposition 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 destinées à l'exploitation d'une organisation, sans lien direct avec l'approvisionnement 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, comptabilité, taxe sur la valeur ajoutée, 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 réglementaires. De même que pour les thèmes spécifiques à la branche énergétique, la gestion des autres données d'une entreprise, comme celles de la comptabilité ou des ressources humaines, doit être représentée.

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

- (1) La mise en œuvre des exigences réglementaires 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 stratégiques en matière de données.

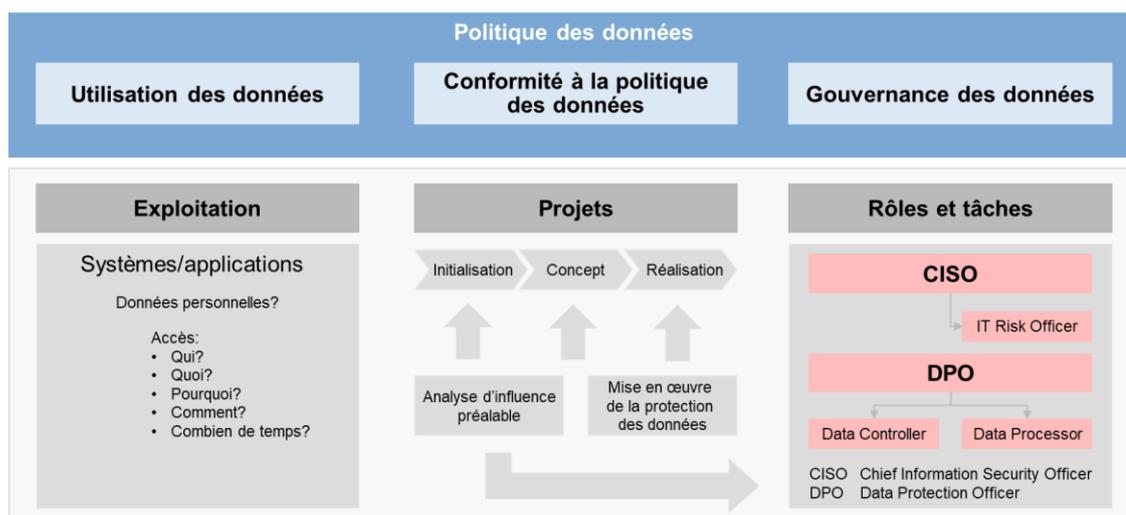


Figure 3 Thèmes abordés dans le cadre de la mise en œuvre de la politique des données

- (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 en matière de protection des données;
 - les exigences en matière de sécurité des données;
 - l'évaluation des conséquences des risques (ainsi que les analyses d'impact relatives à la protection des données (AIPD));
 - l'intégration de la sécurité dès la phase de conception («Security by Design»);
 - la protection de la vie privée dès la phase de conception ou par défaut («Privacy by Design/by Default»).

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) Production, stockage, utilisation, transmission, archivage et suppression: l'ensemble du cycle de vie doit être pris en compte lors de la définition de la gestion des données.
- (6) Dans le cadre de l'exploitation régulière, l'utilisation correcte des données, c'est-à-dire dans le respect des directives relatives à la gestion des données personnelles ou non personnelles, doit être garantie. Toutes les données doivent en principe être classées dans une catégorie et protégées en conséquence. En outre, il convient de garantir les droits des personnes concernées (clients). Les bases relatives au thème de l'utilisation des données sont exposées au chapitre 6 «Recommandations de mise en œuvre de l'utilisation des données».
- (7) Le traitement des données personnelles doit être explicable à tout moment. Les collaborateurs doivent connaître les règles.

4. Fondements juridiques

- (1) Du point de vue spécifique à la branche, les réglementations relatives à l'utilisation des données issues de la séparation au niveau de l'information sont, conformément à l'art. 10, al. 2, LApEI, 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 au niveau de l'information».
- (2) 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 OApEI qui s'appliquent. Ces prescriptions priment les réglementations cantonales relatives à la protection des données. Pour de plus amples explications, cf. section 7.3 «Traitement des données de mesure conformément à l'OApEI».
- (3) Du point de vue juridique, la distinction des données personnelles et non personnelles dans la base de données d'une EAE ainsi que leur finalité d'utilisation sont déterminantes pour un traitement global des thèmes pertinents en matière de données.



4.1 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	OEn
Loi sur l'approvisionnement en électricité	LApEI
Ordonnance sur l'approvisionnement en électricité	OApEI
Règlement général de l'UE sur la protection des données	RGPD
Loi fédérale sur la protection des données	LPD
Lois cantonales sur la protection des données	-
Projet de Loi fédérale concernant la révision totale de la Loi fédérale sur la protection des données et la modification d'autres actes ayant trait à la protection des données ⁴	P-LPD (refonte partielle)
Ordonnance relative à Loi fédérale sur la protection des données	OLPD
Règlement général de l'Union européenne sur la protection des données	RGDP-UE
Ordonnance concernant la tenue et la conservation des livres de compte	Olico

Tableau 2 Vue d'ensemble des réglementations

- (2) Au moment de la création du présent document, les instances législatives ont décidé de procéder au remaniement de la LPD. Sa portée et ses conséquences ne sont pas encore totalement prévisibles à ce jour. L'applicabilité du RGPD-UE pour les activités sur le territoire suisse peut notamment être établie pour le traitement des données personnelles, les services de cloud, etc. transfrontaliers.
- (3) Actuellement, on part du principe que la Suisse dispose, dans le cadre d'un délai transitoire, de quelques années pour parvenir à une régulation équivalente dans le domaine de la protection des données, afin que la décision de l'UE concernant l'adéquation reste positive et qu'un flux de données international ne soit pas assorti d'exigences supplémentaires.
- (4) Le présent document se concentre exclusivement sur le domaine d'application décrit au chapitre 2.

4.2 Données personnelles

- (1) Les régulateurs en Suisse et dans l'UE ont établi une définition descriptive qui n'est pas exhaustive dans la pratique.
- Loi fédérale sur la protection des données (LPD), art. 3, let. a:
Données personnelles (données): toutes les informations qui se rapportent à une personne identifiée ou identifiable.
 - Projet de Loi fédérale sur la protection des données (P-LPD), art. 4, let. a:
Données personnelles: toutes les informations qui se rapportent à une personne physique identifiée ou identifiable.

⁴ Bien que la nouvelle législation sur la protection des données ne soit pas encore entrée en vigueur, le P-LPD a déjà été intégré au présent document afin de mettre en évidence l'évolution future.



- Le règlement général de l'UE sur la protection des données (RGPD-UE) dispose ce qui suit à l'art. 4, al. 1:
Les données à caractère personnel désignent toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»).
- (2) On peut en déduire qu'il existe des données qui peuvent ou doivent être attribuées de façon explicite à une certaine personne (p. ex. nom, prénom, date de naissance). La définition comprend aussi toute forme de données permettant d'identifier une personne (p. ex. par une analyse des données, un profilage). Cette possibilité d'identification peut découler de données et informations quelconques. Dans un contexte correspondant, de telles données et informations sont également soumises à la protection des données.
 - (3) Les processus commerciaux et applications courants dans le cadre desquels 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.

4.3 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, ce n'est pas le cas.
- (2) Le RGPD-UE régit à l'art. 9 le traitement de catégories particulières de données personnelles. La Loi fédérale sur la protection des données définit à l'art. 3, let. c, les données correspondantes et le P-LPD prévoit à l'art. 4, let. c, une définition des données personnelles particulièrement sensibles.
- (3) Les catégories suivantes, particulièrement sensibles, peuvent être déduites par analogie:

Réglementation →	RGPD-UE (état actuel)	LPD CH (état actuel)	P-LPD CH (état prévu)
Catégorie ↓			
Positions et activités religieuses, idéologiques, politiques, syndicales	Oui	Oui	Oui
Données relatives à la santé, la sphère intime*, la race, l'ethnie	Oui	Oui	Oui
Mesures d'aide sociale	Non explicite*	Oui	Oui
Poursuites et sanctions administratives et pénales	Non explicite*	Oui	Oui



Réglementation →	RGPD-UE (état actuel)	LPD CH (état actuel)	P-LPD CH (état prévu)
Catégorie ↓			
Informations génétiques et biométriques	Oui	Non	Prévu
* Peut également comprendre des données relatives à la vie et à l'orientation sexuelles.			

Tableau 3 Catégories de données personnelles particulièrement sensibles

- (4) Les données personnelles particulièrement sensibles sont soumises à des restrictions supplémentaires.

4.4 Données présentant des besoins de protection supérieurs (profilage)

- (1) Lors du recours au profilage (cf. paragraphe 11 du chapitre 5 pour la définition), des mesures techniques et organisationnelles adéquates supplémentaires doivent être prises. Dans le cadre de cette politique des données, la thématique est notamment pertinente pour l'utilisation des systèmes de mesure intelligents («Smart Metering»).
- (2) Le profilage peut aussi s'effectuer différemment, mais il nécessite des obligations d'information et de transparence accrues ainsi qu'une gestion et une protection conformes et adéquates.

4.5 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) Du point de vue de la régulation, le traitement recouvre toutes les actions et activités en lien avec les données et informations, peu importe:
- les médias qui sont utilisés (p. ex. informatique, papier);
 - la manière dont elles sont effectuées: active (p. ex. saisie) ou passive (p. ex. consultation);
 - 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).

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'unité juridique propre ou des tiers, en Suisse ou à l'étranger) n'ont que peu d'importance.

- (3) Le contenu des données et informations et leur gestion occupent le premier plan.
- (4) Une source centrale, consignnant l'ensemble des activités de traitement des données, est essentielle pour assurer le bon déroulement du processus. La nouvelle législation suisse sur la protection des données ainsi que la législation européenne prévoient ce qui suit à cet effet:
- P-LPD Suisse: art. 11 «Registre des activités de traitement»;
 - RGPD-UE: art. 30 «Registre des activités de traitement» (RAT).
- (5) Les données et informations peuvent être soumises à d'autres restrictions réglementaires encore, telles que les directives de séparation des activités (conformément à la LApEI et à l'OApEI), les directives du droit de la concurrence et/ou des cartels 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.

4.6 Gestion des données des personnes morales

- (1) Si les données des personnes morales sont soumises à l'actuelle LPD, elles sont exclues du RGPD-UE et de la future Loi fédérale sur la protection des données (P-LPD).

5. 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

On entend par ce terme la protection des données personnelles contre l'abus, souvent dans le contexte de la protection de la sphère privée. La finalité et l'objectif de la protection des données sont 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) Sécurité des données

Ensemble des mesures techniques et organisationnelles visant à garantir la sécurité physique et logique. Il s'agit en priorité de protéger les données contre l'accès non autorisé, la modification et la perte afin de garantir leur disponibilité et leur intégrité.

(4) 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.

(5) 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 6.2, paragraphe 3.



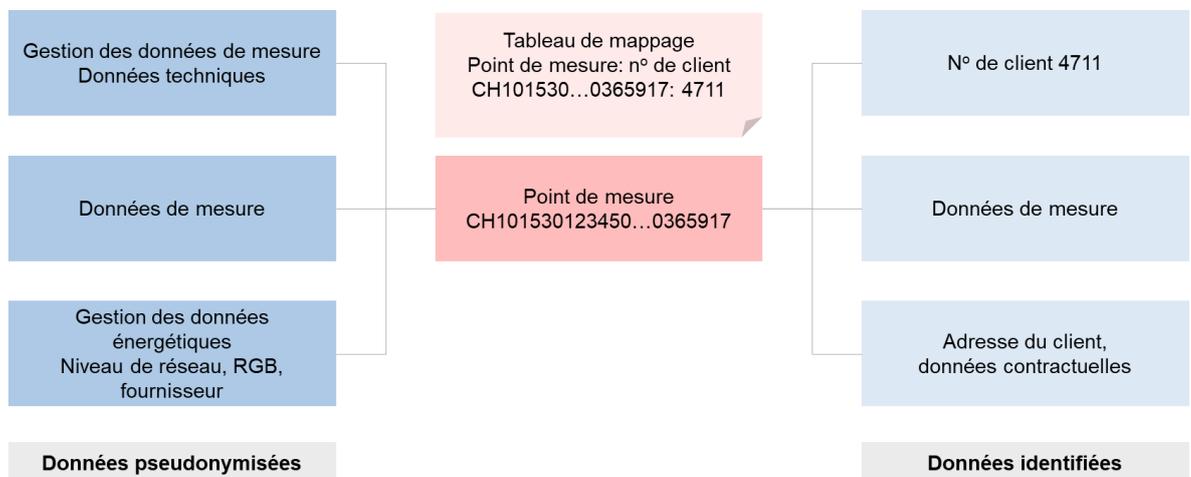


Figure 4 Exemple de mise en œuvre de la pseudonymisation avec un tableau de mappage

(6) 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 complexes. 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:

- Plusieurs⁵ 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.

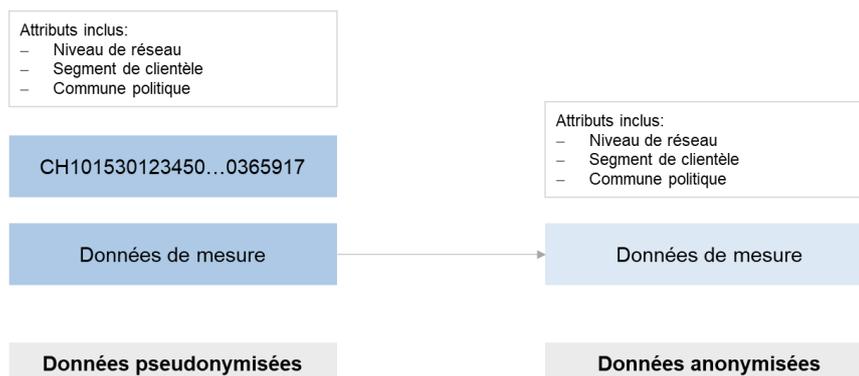


Figure 5 Exemple de mise en œuvre de l'anonymisation

(7) Données personnelles au sein de l'EAE

Les données personnelles sont par exemple des données issues de systèmes de mesure intelligents, des données de mesure d'installation, de programme prévisionnel et de pronostics, des signaux de

⁵ 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.



commande et d'incitation, et des données clients, contractuelles ou d'électromobilité. Des informations approfondies sont disponibles à l'annexe «Conformité à la politique des données – modèles de données et applications».

(8) **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 à l'annexe «Conformité à la politique des données – modèles de données et applications».

(9) **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. 6 et 7 P-LPD).

(10) **Privacy by Design/by Default**

Pour la protection des données personnelles, les principes s'appliquent par analogie, comme cela est décrit à la rubrique «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.

(11) **Profilage («Profiling»)**

Utilisation de données personnelles pour créer, actualiser ou utiliser des profils sur l'individu à l'aide d'analyses et d'évaluations. Les résultats sont souvent exploités à des fins de conception de produit ou de marketing.

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 réglementaires (étrangères) complémentaires s'appliquent. Cf. aussi 4.1 (2).

6.1 Séparation au niveau de l'information

- (1) La séparation des activités («Unbundling») désigne la distinction entre l'exploitation du réseau et les autres secteurs d'activité d'une EAE (art. 10, al. 2, LApEI: «*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 la vente d'énergie, le conseil en énergie, l'installation et 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.
- (2) Les données des utilisateurs du réseau sont en général considérées comme des **informations économiquement sensibles**, car le gestionnaire de réseau peut se ménager un avantage concurrentiel avec les informations obtenues. 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 à la charge ou aux dépens et sur la base d'informations issues de l'exploitation du réseau ou de l'approvisionnement de base (cf. section 6.1, 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) Les données déterminantes pour le décompte et la rétribution (cf. définition à la section 7.3 «Traitement des données de mesure conformément à l'OApEI») ne sont pas pseudonymisées exclusivement 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 visible que par les personnes autorisées (en interne ou en externe) exécutant des processus pertinents pour le décompte et la rétribution. Cf. annexe «Conformité à la politique des données – données issues de l'exploitation du réseau et de l'approvisionnement de base».

- (4) Conformément à la Stratégie énergétique 2050, les dispositifs de mesure seront transformés en systèmes de mesure intelligents dans les prochaines années. Dès lors qu'un tarif d'utilisation du réseau basé notamment sur une composante de courbe de charge est appliqué pour un client, la courbe de charge est pertinente pour le décompte et la rétribution et elle doit en principe être utilisée de façon non pseudonymisée uniquement pour le processus de décompte. Si la courbe de charge du client est disponible dans le cadre de la gestion des données de mesure (GDM) et de la gestion des données énergétiques (GDE) et que seule la quantité mensuelle, p. ex., est décomptée dans le système de mesure, seule cette valeur agrégée de la GDM ou de la GDE est transmise au système de décompte.
- (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 réelles 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 du GRD

- (1) L'utilisation de systèmes de mesure intelligents doit favoriser l'innovation, les potentiels d'économie d'énergie et le développement de nouveaux modèles commerciaux. Afin d'exploiter le potentiel de tels systèmes, une utilisation des données plus large que les domaines d'application définis à l'art. 8d LApEI est possible avec l'accord du client final (opt-in). L'utilisation élargie des données est possible si l'utilisateur du réseau donne son consentement explicite, conforme à la séparation des activités et dans un but précis, et ce, selon la formulation contenue dans le consentement.



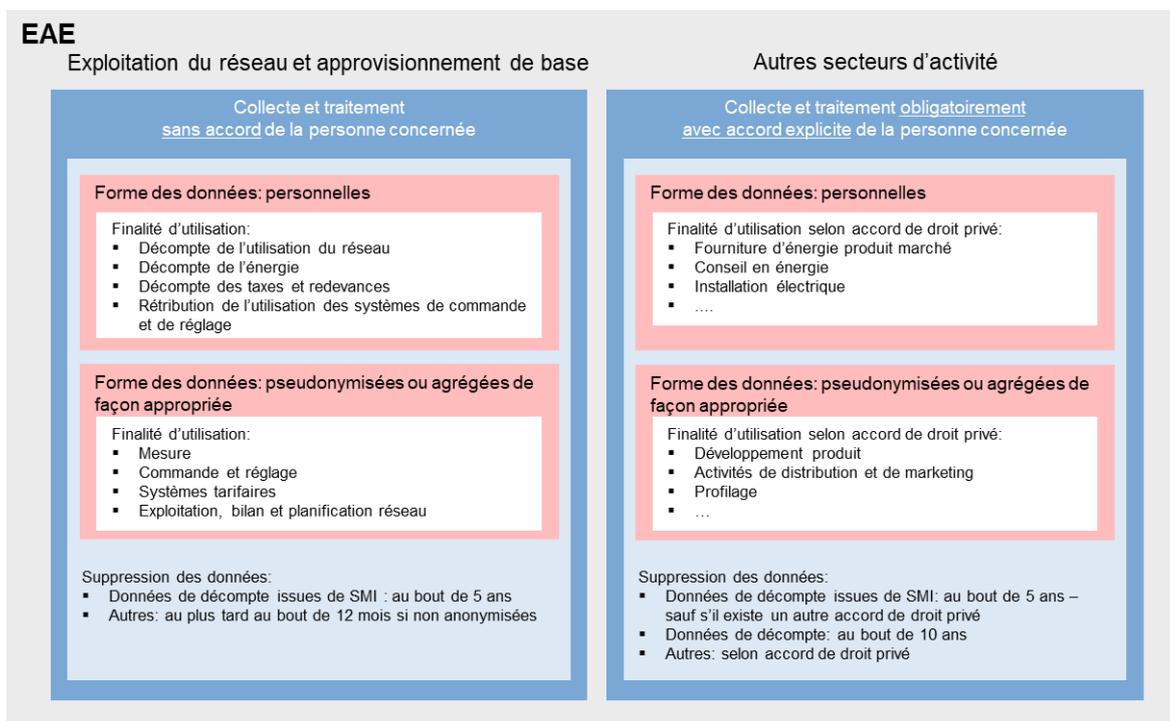


Figure 6 Utilisation des données issues de SMI (art. 8d OApEI) en lien avec la séparation au niveau de l'information (art. 10, al. 2, LApEI)

6.4 Autres secteurs d'activité

- (1) Pour l'utilisation des données dans les autres secteurs d'activité de l'EAE, une réglementation/base juridique est nécessaire.

6.5 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 réglementaires pertinentes (pour les contrats existants et nouveaux). Les tiers 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 systèmes de cloud, des administrateurs système d'un partenaire d'externalisation et des collaborateurs support d'un concepteur de logiciels. Toute unité juridique différente de l'unité juridique qui collecte/traité les données doit être considérée comme un tiers du point de vue du droit de la protection des données. Ce principe s'applique également au sein des groupes de sociétés.



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

- (1) La conformité à la politique des données⁶ 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 l'Ordonnance sur l'approvisionnement en électricité (art. 8 et 8d OApEI) et l'Ordonnance relative à la Loi fédérale sur la protection des données (art. 8 à 10 OLPD).
 - Les fondements de la garantie de la conformité à la politique des données sont décrits au chapitre 6 du rapport sur la politique des données dans le secteur énergétique. 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) Dans le présent chapitre, on entend par «protection des données» la protection des données sur la base de la LPD, mais aussi la gestion des données d'entreprise critiques sur la base des réglementations internes à l'entreprise.
- (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 restrictions, mesures et protections techniques et organisationnelles 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.
- (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, 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 de la section 4.5 «Traitement des données», diverses bases légales

⁶ Aussi appelé «compliance»



s'appliquent aux données citées. En principe, toutes les données peuvent être saisies et consignées dans le registre des activités de traitement (RAT). Cf. à ce sujet la section 8.3.

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, autrement dit la criticité, des objets de données. Des mesures en seront déduites dans un second temps. Cf. à ce sujet la section 6.2 du rapport sur la politique des données dans le secteur énergétique.
- (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 = Accountability = Traçabilité

Il en résulte une analyse CIA-AAA complète.

7.3 Traitement des données de mesure conformément à l'OApEI

- (1) Art. 8d «Traitement des données enregistrées au moyen de systèmes de mesure, de commande et de réglage intelligents», al. 3, OApEI:
«Les données personnelles et les profils de la personnalité sont détruits au bout de douze mois s'ils ne sont pas déterminants pour le décompte ou anonymisés.»
 - En principe, les données doivent être supprimées au bout de douze mois.
 - Il est autorisé de stocker les données pour une plus longue durée lorsqu'elles sont déterminantes pour le décompte.
 - Il existe en outre la possibilité de stocker les données plus longtemps que douze mois lorsque les utilisateurs du réseau y consentent explicitement (opt-in). L'accord doit alors contenir l'objectif d'utilisation. Il peut être révoqué à tout moment. Cela devrait à l'avenir être ancré dans la loi. Voir à ce sujet l'art. 5, al. 3, 4 et 6, l'art. 6, al. 3, ainsi que l'art. 27, al. 2, let. a et e, P-LPD.
 - Il existe la possibilité d'anonymiser les données pour les stocker plus longtemps. Dans ce cas, les données ne peuvent cependant plus être utilisées pour satisfaire l'obligation de renseigner selon l'art. 8, al. 3, OApEI, car l'attribution à un utilisateur du réseau n'est plus possible.
- (2) Les données sont déterminantes pour le décompte lorsqu'elles servent à établir les décomptes pour l'utilisateur du réseau ou à garantir la gestion du bilan d'ajustement ou l'obligation de renseigner conformément à l'art. 8, al. 3, OApEI. Peu importe qu'il s'agisse de données de la courbe de charge (par tranche de 15 minutes au maximum) ou d'états des compteurs.



- Les données issues de systèmes de commande et de réglage intelligents ainsi que celles qui sont exclusivement visualisées sur un portail client ne sont pas considérées comme déterminantes pour le décompte. Dans de tels cas, les données doivent être supprimées au plus tard au bout de douze mois en l'absence d'accord explicite de la part de l'utilisateur du réseau. D'autres délais peuvent être convenus contractuellement. Une durée de conservation plus longue peut également constituer un avantage pour les clients, p. ex. pour suivre les mesures d'économie d'énergie.
- Les données déterminantes pour le décompte doivent être conservées pendant cinq ans (art. 8, al. 4, OApEI: «*Tous les chiffres relevés au cours des cinq années précédentes doivent être livrés.*»). Les données doivent ensuite être supprimées ou transformées sous une forme anonymisée ou agrégée appropriée (cf. section 7.1, paragraphe 1, points 1 et 2).

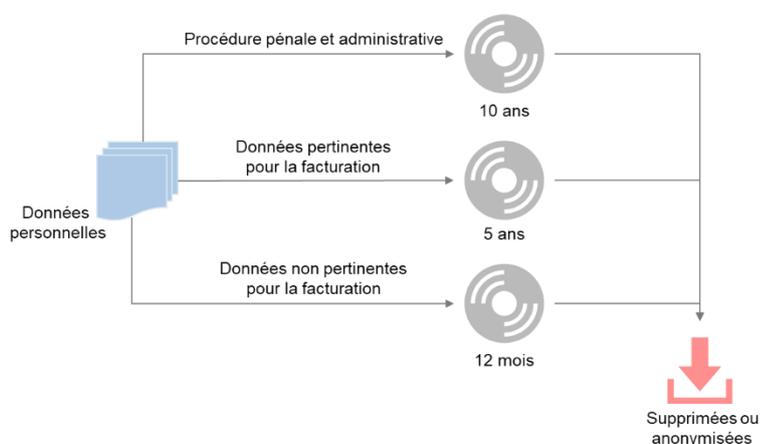


Figure 7 Directives relatives à l'obligation de conservation des données personnelles

- (3) Art. 8 «Système de mesure et processus d'information», al. 4, OApEI:
 «*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.*»
- Pour la transmission de données et informations supplémentaires, l'accord de l'utilisateur du réseau est nécessaire.
- (4) Le message relatif à la révision totale de la LPD décrit les détails concernant l'intérêt supérieur de la personne chargée du traitement conformément à l'OApEI. Par dérogation, on cite explicitement le délai de douze mois au lieu de l'art. 4 «Principes», al. 4, LPD: «*Elles sont détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement.*»
- L'intérêt supérieur peut différer de cette réglementation.
 - Les réglementations divergentes relèvent de la responsabilité du GRD. Il est recommandé d'établir une documentation détaillée relative à la garantie de la conformité à la politique des données.



- (5) Les entreprises doivent assurer une gestion du cycle de vie pour toutes les bases de données. Cela comprend p. ex. la conservation, l'archivage, la suppression et le renseignement (cf. paragraphe 4 de la section 4.5 «Traitement des données»).

7.4 Gestion approfondie des données personnelles

- (1) Pour toute forme d'utilisation approfondie des données, p. ex. pour le profilage ou la transmission de données à des tiers, il faut en principe faire la distinction entre les clients captifs (clients dans l'approvisionnement de base) et les clients disposant de contrats de droit privé. L'absence d'alternative pour les clients captifs est alors déterminante.
- **Clients captifs:** un accord explicite doit exister pour toute réutilisation des données. Une réglementation correspondante dans les CGV n'est donc **pas suffisante**.
 - **Clients disposant de contrats de droit privé:** la réutilisation des données doit être réglée par contrat (c.-à-d. par un accord explicite 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 LApEI est **suffisante** du point de vue juridique.
L'art. 8d OApEI, en vigueur depuis le 1^{er} 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) Dans le cadre d'un traitement des données en dehors de l'unité juridique propre (tiers, autre unité juridique au sein d'un groupe), les fondements juridiques déterminants doivent être pris en compte.
- (3) Par analogie avec le traitement externe, le traitement et la conservation des données à l'étranger doivent être déclarés dans le contrat ou les CGV avec le client. 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 données⁷ et que le niveau nécessaire ne peut pas non plus être garanti d'une autre façon (p. ex. US Privacy Shield, bouclier de protection des données États-Unis), il faut en outre recueillir l'accord explicite du client et prendre des mesures techniques et organisationnelles complémentaires. Cf. à ce sujet l'art. 6 LPD.
- (4) 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'OApEI. Cf. à ce sujet la section 7.3. «Traitement des données de mesure conformément à l'OApEI».
- (5) Selon la révision de la Loi fédérale sur la protection des données, les clients qui souhaitent des renseignements concernant leurs données personnelles doivent pouvoir se tourner vers un bureau de

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, 1^{er} al., LPD)»



coordination. Le client a le droit d'obtenir des renseignements sur les données qu'il traite. Le préposé fédéral à la protection des données met un formulaire standard à disposition. Il faut en principe répondre aux demandes de renseignements gratuitement dans les 30 jours. Dans certains cas, les clients peuvent exiger une régularisation, un blocage ou une suppression de leurs données. Des droits et obligations supérieurs sur le plan juridique et réglementaire restent réservés.

7.5 Gestion des données non personnelles

(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 sont concernées, la législation sur la protection des données s'applique et la gestion des données doit s'effectuer conformément aux directives correspondantes. À ce sujet, cf. aussi section 4.6 «Gestion des données des personnes morales».

(3) Données SCADA

Si des personnes physiques ou morales sont concernées, la législation sur la protection des données s'applique et la gestion des données doit s'effectuer conformément aux directives correspondantes. À ce sujet, cf. aussi section 4.6 «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.

Modèle de données

- (2) Pour les EAE qui opèrent surtout en tant qu'exploitantes du réseau, un modèle de données simplifié 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 à l'annexe «Conformité à la politique des données – modèles de données et applications».

- (3) La protection des données s'étend aux données personnelles ainsi qu'aux données visant à garantir la sécurité d'approvisionnement:

- 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.
- 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 à l'annexe «Conformité à la politique des données – modèles de données et applications».

Définition des besoins de protection

- (4) Le paysage des applications d'une EAE petite à moyenne est décrit à l'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.

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

Garantie des besoins de protection et des responsabilités

- (5) 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 création ainsi que de la surveillance régulière des menaces, risques et mesures doit être réglée pour toutes les EAE. Dans une petite EAE, les diverses tâches peuvent être assumées par une même personne. La responsabilité lors du recours à des tiers pour certaines activités 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 pour fixer, mettre en œuvre, entretenir et développer durablement les réglementations de la politique des données. Les tâches, rôles, comités et processus de gouvernance nécessaires sont en outre déterminés.
- (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.



(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 de ces dernières est établi et entretenu. Cf. à ce sujet le paragraphe 4 de la section 4.5. «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 réglementaire 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 réglementaire 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) Pour la réalisation des tâches relevant de l'utilisation et de la gouvernance des données, ainsi que de la conformité à la politique des données, l'introduction des rôles suivants est recommandée.
- (2) En fonction de la taille de l'organisation, une même personne peut assumer plusieurs rôles. Dans les petites entreprises, la direction peut remplir certaines de ces fonctions. Dans les grandes entreprises, ces rôles peuvent être clairement définis et attribués à différentes personnes. La séparation des pouvoirs doit être garantie.

Abré- viation	Désignation des rôles et des fonctions	Description des tâches possibles
DPO	Data Protection Officer / délégué à la protection des données / responsable de la protection des données	Compétent et responsable pour toutes les questions au sein de l'entreprise relevant de la Loi fédérale sur la protection des données (Droit fondamental relatif à la protection de l'auto-dé- termination en matière d'information) Tâches possibles: – Création et mise à jour du registre des procédures – 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



Abré- viation	Désignation des rôles et des fonctions	Description des tâches possibles
		<ul style="list-style-type: none"> – Conclusion d'accords portant sur le traitement (des données) des mandats 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 – Réponse aux demandes de renseignements des personnes concernées ou des autorités de surveillance en ce qui concerne le traitement/stockage des données personnelles
CISO	Chief Information Security Officer / chef de la sécurité des informations	<p>Compétent pour la sécurité logique des informations d'une organisation</p> <p>Tâches possibles:</p> <ul style="list-style-type: none"> – 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
CSO	Chief Security Officer / chef de la sécurité	<p>Compétent et responsable pour toutes les questions relatives à la sécurité physique (bâtiments, clés, accès...)</p> <p>Tâches possibles:</p> <ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – 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



Abré- viation	Désignation des rôles et des fonctions	Description des tâches possibles
		du non-respect de dispositions (législatives ou régula- toires) spécifiques, de normes professionnelles ou éthiques ou d'instructions de l'organe exécutif – Fonction d'information, de formation et de conseil, aussi bien pour les collaborateurs que pour la direction de l'en- treprise

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 approfondie.
- (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:

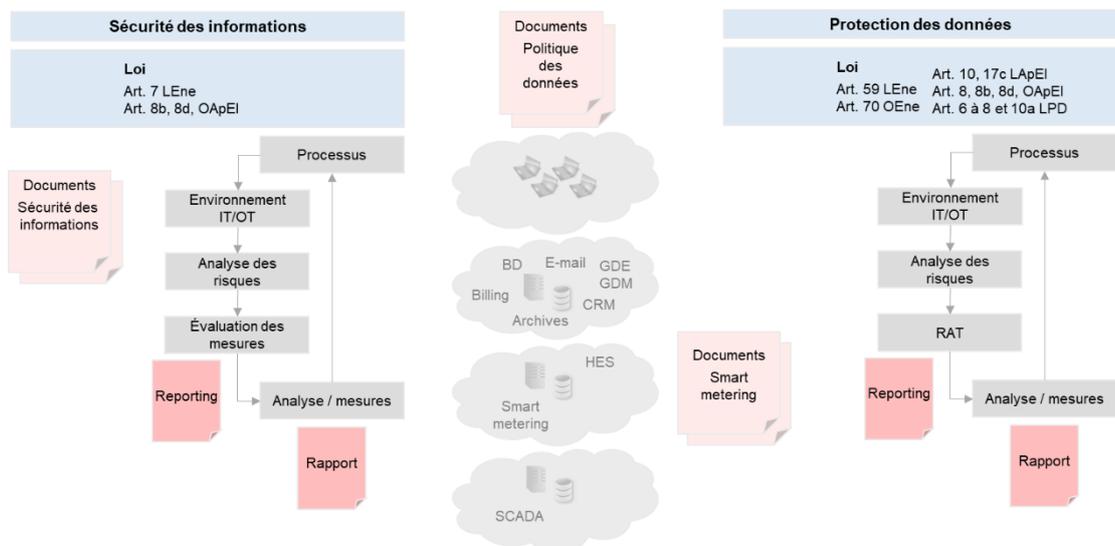


Figure 8 Interaction entre la sécurité des informations et la protection des données

- Un environnement informatique simplifié peut p. ex. regrouper un environnement SCADA, un environnement de metering, un environnement de traitement des données et l'environnement constitué par les ordinateurs.
- 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 DPO 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 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 4.5 «Traitement des données».
- (2) Le RAT donne des renseignements sur tous les aspects essentiels de la gestion 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 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 interdomaines, un traitement et une mise à jour.
- (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 réglementation de «best practice». Voir aussi la section 6.2.1 du rapport 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).
- (6) La structure recommandée pour le RAT est consultable à l'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 clients d'une EAE sont majoritairement des personnes physiques. Les données suivantes de ces individus font l'objet d'une gestion et d'un traitement (liste non exhaustive):
- Données client
 - Nom, prénom
 - Adresse
 - Bâtiment
 - Données contractuelles
 - Contrats de fourniture d'électricité et de raccordement au réseau avec durée de validité (jusqu'à l'ouverture complète du marché, il s'agit majoritairement de contrats intégrés pour le réseau et l'énergie).
 - 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 nécessaire (par tranche de 15 minutes)
 - Éventuellement valeurs 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 (par tranche de 15 minutes au maximum)
 - Données d'installation
 - Récepteur de télécommande avec commandes utilisées
- (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 (par tranche de 15 minutes au maximum)
 - 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

Description du paysage des applications d'une EAE petite à moyenne

- (5) 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. Les deux systèmes sont majoritairement exploités de façon autonome par l'EAE.
- (6) Le relevé des compteurs à distance (aussi bien traditionnel que via un système de smart metering) 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.
- (7) 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, qui sera probablement majoritairement mise en œuvre par les prestataires.
- (8) 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.



- (9) Un système SCADA est rarement disponible ou l'est seulement sous une forme très réduite, p. ex. à des fins de mise en alerte.



Détails → Catégorie ↓	Formes possibles	Thématiques possibles	Remarques
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, le traitement (des données) des mandats 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 5 «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.



Description générale des mesures techniques et organisationnelles (MTO)	
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. Glossaire

Abréviation	Description
A	Availability / Authentication / Authorization / Accountability
AES	Association des entreprises électriques suisses
BD	Base de données
C	Confidentialité
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
DPO	Data Protection/Privacy 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)
I	Intégrité
ISO	Organisation internationale de normalisation
IT	Information Technology (technologies de l'information, informatique)
LApEI	Loi sur l'approvisionnement en électricité
LEne	Loi sur l'énergie
LPD	Loi fédérale sur la protection des données
MTO	Mesures techniques et organisationnelles
OApEI	Ordonnance sur l'approvisionnement en électricité
OEné	Ordonnance sur l'énergie
OLEI	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
PPFDT	Préposé fédéral à la protection des données et à la transparence
P-LPD	Projet relatif à la Loi fédérale sur la protection des données
RAT	Registre des activités de traitement
RCD	Relevé des compteurs à distance



Abréviation	Description
RGPD-UE	Règlement général de l'Union européenne sur la protection des données
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

