protendo
proteggi conoscendo

Sommario

1. DPIA

Il Data Protection Impact Assessment (DPIA) è un processo volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche, effettuando una valutazione del livello di tali rischi e determinando le misure idonee a mitigarli.
Il DPIA va inquadrato come uno strumento essenziale e fondamentale per tutti i titolari e responsabili del trattamento al fine di dar corso al nuovo approccio alla protezione dei dati personali richiamato dal GDPR, fortemente basato sul principio di accountability.
Un processo di DPIA può riguardare una singola operazione di trattamento dei dati.
Tuttavia si potrebbe ricorrere a un singolo DPIA anche nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi.
Ciò potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità.
Oppure, un singolo DPIA potrebbe essere applicabile anche a trattamenti simili attuati da diversi titolari del trattamento dei dati.
In questi casi, è necessario condividere o rendere pubblicamente accessibile un DPIA di riferimento, attuare le misure descritte nello stesso e fornire una giustificazione per la realizzazione di un unico DPIA.

2. QUANDO SI EFFETTUA LA DPIA

L’art. 35 del GDPR stabilisce che è necessario effettuare una DPIA in tutti i casi in cui le operazioni di trattamento presentano rischi elevati per i diritti e le libertà delle persone fisiche in virtù della loro natura, portata o finalità o quando possono procurare un danno economico o sociale importante.
La DPIA deve essere effettuata prima di procedere al trattamento, già dalla fase di progettazione del trattamento stesso anche se alcune delle operazioni di trattamento non sono ancora note, in coerenza con i principi di privacy by design e by default per determinare se il trattamento deve prevedere misure opportune in grado di mitigare i rischi.
L'aggiornamento della valutazione d'impatto sulla protezione dei dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità.
La valutazione DPIA concorre quindi, insieme ad eventuali altri processi di valutazione e gestione del rischio (es. Gestione del rischio in ambito ISMS) alla “Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita” come previsto dall’art. 25 del GDPR.
Ciò consente di acquisire le necessarie conoscenze sulle misure, garanzie e meccanismi da prevedere per mitigare il rischio e assicurare la conformità del trattamento al GDPR, prima che possano essere arrecati danni ai diritti ed alle libertà delle persone fisiche. Al fine di garantire la corretta attivazione di un processo di DPIA è bene definire alcuni punti di

attenzione in cui valutare appunto la necessità di realizzare o meno un Privacy Impact Assessment:

- Introduzione di nuovi trattamenti nell'ambito di nuovi processi e/o nuove attività aziendali;
- Importanti revisioni del modello organizzativo, con effetti su processi e relativi trattamenti;
- Nuovi servizi informativi e/o modifica dei servizi informatici in essere a supporto di trattamenti esistenti;
- Variazioni significative ai trattamenti in essere.

Anche se il regolamento evidenzia l'applicazione della valutazione di Impatto per i nuovi trattamenti, è comunque consigliabile (suggerito anche dalla linea guida WP248) valutare anche i trattamenti in corso prima del 25 maggio 2018 arrivando comunque a determinare la loro conformità al GDPR e la necessità o meno di effettuare una DPIA.

3. ESEMPIO PRATICO - I CONTATORI INTELLIGENTI

I contatori intelligenti (smart meter) sono dispositivi che aiutano consumatori e fornitori ad adattare il loro utilizzo di energia (in termini di tempo e volume) fornendo informazioni sul consumo di energia in tempo reale.
Attraverso l'inverter x, applicativo in grado di verificare l'energia prodotta in un giorno, è possibile decidere autonomamente quando e quali apparecchi domestici attivare e disattivare, semplicemente sfruttando una rete mobile o connessione Internet.
L'utilizzo di tali strumenti è innovativo su diversi fronti, dal risparmio energetico al controllo dei propri consumi, ma comporta diverse attività di trattamento, fino ad arrivare alla raccolta di informazioni e nello specifico di **dati personali** in quanto **ogni dispositivo è riconducibile facilmente a un cliente.**
Ciò che interessava al fine del Regolamento UE 679/2016, è che il modo in cui l'utente finale utilizza l'energia, che viene rilevato dal fornitore tramite lo Smart Meter, può avere un impatto sulla vita del consumatore, non solamente in termini di costo (e quindi di bolletta), ma anche sulla quantità di energia erogata, raccogliendo ed elaborando informazioni derivanti dai dispositivi.
Analizzando dettagliatamente tali dispositivi si rileva ai fini giuridici che:

a) Il trattamento tramite Inverter intelligenti ricade nell'ambito delle procedure per le quali l'art. 35 GDPR ed il successivo Provvedimento n. 467 dell'11 ottobre 2018 del nostro Garante prevedono **l'obbligatorietà della DPIA**.
A tale riguardo:

- la Commissione Europea ha istituito una Task Force per le Smart Grids, composta da cinque gruppi di esperti che si concentrano su diverse aree specifiche.
  Uno di questi, Expert Group 2, ha il compito di mitigare il rischio sulla privacy e sulla sicurezza dei sistemi di misurazione intelligente.
  Il Gruppo di lavoro ha predisposto apposita DPIA di esempio (vedi allegato 2) sui trattamenti che possano rilevare il consumo energetico.

- l'autorità belga (prima autorità Garante ad esprimersi in merito) ha incluso tra i trattamenti per cui la valutazione di impatto deve ritenersi obbligatoria, il trattamento inerente l'elaborazione su larga scala di dati generati da dispositivi dotato di sensori che inviano dati via Internet o altri mezzi (Internet of Things, come smartTV, elettrodomestici intelligenti, giocattoli, smart cities, contatori intelligenti di energia, ecc.) e tale trattamento viene utilizzato per analizzare o prevedere la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, la posizione o il movimento delle persone fisiche;

b) ai sensi dell'articolo 29 del GDPR, i Clienti hanno il diritto di passare da un fornitore di servizi ad un altro e allo stesso tempo decidere quale quantità di dati trasferire ai nuovi fornitori di servizi e quale quantità di dati dimenticare (diritto alla portabilità dei dati e all'oblio).

c) Sarà necessaria la designazione del DPO.
Ai sensi dell'art. 37, primo paragrafo, del GDPR, la designazione del dpo è obbligatoria in tre ipotesi:

- se il trattamento di dati personali è effettuato da un'autorità pubblica o da un organismo pubblico,
- quando le attività principali dell'organizzazione consistono in trattamenti che, richiedono il "monitoraggio regolare e sistematico" degli interessati "su larga scala";
- quando le attività principali dell'organizzazione consistono nel trattamento "su larga scala" di dati "sensibili" ("categorie particolari di dati") o "giudiziari" ("dati personali relativi a condanne penali e reati").

In virtù di quanto sopra, per verificare se sono o meno soggette all'obbligo di nominare un Data Protection Officer ai sensi dell'art. 37, par. 1, lett. b), l'impresa dovrà valutare:

- ✓ se le attività di trattamento effettuate, per loro natura, ambito di applicazione e/o finalità, richiedono un "monitoraggio regolare e sistematico" degli interessati;
- ✓ in caso affermativo, se tale monitoraggio è effettuato "su larga scala";
- ✓ infine se tale monitoraggio si può considerare "attività principale".

Vediamo come applicare questi criteri in concreto con un esempio pratico:

Un'azienda nei settori idrico, energetico e gas, con diversi utenti in svariati Comuni di alcune Regioni italiane, monitora in maniera costante e regolare i consumi dei propri utenti, consente loro di effettuare l'autolettura a distanza, in automatico, dei consumi di acqua, luce, gas e fornisce servizi web di analisi dei consumi.
A prescindere dall'applicabilità del criterio di cui all'art. 37, primo paragrafo, lett. a), è sostenibile che tale società effettui un'attività di monitoraggio degli interessati in maniera regolare e sistematica in base all'interpretazione di tali aggettivi fornita dal WP29 e che il trattamento di dati dalla stessa effettuato, dato il numero di soggetti coinvolti, la quantità di dati trattati, la durata e l'estensione geografica delle attività di trattamento, si possa anche considerare,

ai sensi del considerando 91, un trattamento di “una notevole quantità di dati personali a livello regionale” e, quindi, su “larga scala”.
Per quanto concerne l’ultima caratteristica, l’“attività principale” svolta da tale società non è il trattamento dei dati personali dei propri utenti, ma la fornitura di servizi.
Bisogna quindi valutare se sia possibile erogare efficacemente tali servizi senza trattare dati personali.
Fra gli esempi riportati dal WP29 non è ricompresa espressamente l’ipotesi di società che forniscono un tale tipo di servizi, ma non si può escludere che la rilevazione costante dei consumi possa essere ritenuta necessaria per erogare tali servizi o legata in modo inscindibile all’attività principale della società.
Appare opportuno, pertanto, che tale società nomini un DPO.

4. RIFERIMENTI NORMATIVI ED ALLEGATI

- Regolamento Europeo 679/2016
- Provvedimento n. 467 dell’11 ottobre 2018 del nostro Garante. Allegato 1
- dpia_for_publication_2018. Allegato 2

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

***CHIARIMENTO INTERPRETATIVO**

ALLEGATO 1 AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018 [doc. web n. 9058979]

(Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018)

Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto

1. Trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad *"aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato*".

2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "*effetti giuridici*" oppure che incidono "*in modo analogo significativamente*" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).

3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi *web*, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di *budget*, di *upgrade* tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).

6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*; tracciamenti di prossimità come ad es. il *wi-fi tracking*) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .

8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. *mobile payment*).

10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Smart Grid Task Force 2012-14

Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment

Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems

v. 2 of 13 September 2018

Contents

1. Introduction

1.1. About the Template

The present Data Protection Impact Assessment (DPIA) Template for Smart Grid and Smart Metering Systems is composed of three parts:

- **Introductory Part in Chapter 1**

This part provides information about the development of the Template, its nature and scope of application. It provides context necessary to understand the process of the DPIA in the Smart Grids' environment, its legal and business conditioning as well as relevant terminology.

- **Explanatory Part in Chapter 2**
- **Questionnaire in Chapter 3**

The Questionnaire is the operative part of the Template to be used by Smart Grids and Smart Metering systems' operators in the DPIA process. The Questionnaire is mirrored in the Explanatory Part – i.e. every element of Chapter 3 is explained by a corresponding entry in Chapter 2. Having Chapter 2 and Chapter 3 presented side by side (with two screens or with two printed copies) will facilitate the understanding of the DPIA process and streamline its accomplishment.

1.2. Development and Adoption Framework

The editorial team responsible for the Template was composed of industry representatives involved in the Smart Grid Task Force (SGTF) – a stakeholders' platform that involves regulators and other competent authorities, consumers, suppliers, traders, power exchanges, transmission companies, distribution companies, power equipment manufacturers, standardisation organisations and ICT products and service providers. The SGTF was set up by the European Commission in 2009 to advise on issues related to Smart Grid deployment and development as well as to facilitate co-ordination of policy and regulatory best practices at European level. The SGTF consists of a steering committee (SC) and five expert groups (EGs) that focus on specific areas. The SGTF issues key recommendations for standardisation, consumer data privacy and security. The Development of this Template lies within the mandate of the SGTF's EG 2 which is dedicated to the identification of the appropriate regulatory scenarios and recommendations for data handling, data security and data protection. This task is aimed at establishing a data privacy and data security framework that both protects and enables. EG 2 adopts regulatory recommendations for Privacy, data protection and cyber-security in the Smart Grid environment.

The first Template was submitted on 8th of January 2013 to the Article 29 Working Party (WP 29)[1] for consultation, in accordance with point 5 of the Recommendation adopted by the Commission on the

[1] The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data.

roll out of Smart Metering Systems[2]. The WP29 issued its opinion on 22nd of April 2013 recommending a series of changes and improvements in order for the Template to be satisfactory. The second DPIA Template was submitted on 20th of August 2013 to the WP29 for consultation. On 4th of December 2013 the WP29 issued a second opinion recognising the work carried out by the EG 2 and realising that the second version of the Template constitutes considerable improvement with respect to the previous version especially with regard to the methodology used. The WP29 provided as well complementary recommendations which will contribute to the successful deployment and use of the Template. The third version of the DPIA Template has been prepared by an editorial team which has constructively addressed WP29 last recommendations and has been finalised by the EG2 members on 10th of March 2014

The origin of this version of the Template dates back to the Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems that planned for a two year test phase of the DPIA Template to gather feedback[3] amongst stakeholders. For over two years the Commission has facilitated the test phase and the subsequent reviewing and enhancements on the Template. The EG 2 has worked on the Template in order to accommodate feedback and experience gathered during the test phase and adopted the present fourth version of the Template.

The current version of the Template has been extensively updated due to the adoption of the General Data Protection Regulation (GDPR)[4] which becomes applicable as of 25 May 2018. Since the DPIA becomes mandatory in certain circumstances this Template could serve as a model for future DPIAs in the sector. All the notions applied in this Template should have the meaning assigned thereto in the GDPR, unless otherwise provided.

Development of this version of the Template has been facilitated by the European Commission's assessment team and submitted to the Article 29 Working Party for information[5].

1.3. Purpose of the Template

The Data Protection Impact Assessment Template is destined for Data Controllers that are Smart Grid operators that manage or initiate Smart Grids or Smart Metering Systems, as well as those that introduce changes to existing Smart Grid architecture platforms. Since the collection and usage of Personal Data (e.g., household consumption, usage data) is one of the key business enablers for Smart Grid operators, the inherent Risks to the rights and freedoms of natural persons[6] (Data Subjects) shall

[2] The Recommendation 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart metering systems**,** OJ L 73, 13.3.2012, p. 9–22.
[3] OJ L 300, 18.10.2014, p. 63–68.
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.
[5] The Recommendation 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart metering systems announced the development of a Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, to be submitted for opinion to the Article 29 Working Party on the protection of individuals with regard to the processing of Personal Data.
[6] Recital (75) of the GDPR

be properly assessed and mitigated and the rules for collecting Personal Data should be established, in particular with regard to proportionality of collection to the purpose of processing and legal basis.

This document will guide Data Controllers in conducting a thorough DPIA which describes the envisaged Data Processing, an assessment of the Risks to the rights and freedoms of data subjects, the measures, safeguards, Controls and mechanisms envisaged to address the Risks, ensuring the protection of Personal Data[7].

The GDPR foresees the DPIA as a key instrument to enhance Data Controllers' accountability as it helps controller not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the GDPR. In other words, a DPIA is a process for building and demonstrating compliance[8].

The GDPR makes it mandatory to perform a DPIA when Data Processing is likely to result in a high Risk to the rights and freedoms of natural persons. Be advised that although carrying out a DPIA is not always mandatory, compliance with other GDPR Requirements has to be assured at all times irrespectively of the DPIA execution.

The GDPR (art. 35.3) laid down three types of Data Processing operations classified as requiring a DPIA:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) processing on a large scale of special categories of data referred to in Article 9(1) GDPR, or of Personal Data relating to criminal convictions and offences referred to in Article 10 GDPR; or
(c) a systematic monitoring of a publicly accessible area on a large scale[9].

Additionally, the Data Protection Authorities (DPAs) will establish lists of the kind of processing operations requiring a DPIA and, in the case where the processing is cross-border, the list of processing operations of the DPAs will go through the consistency mechanism[10].

A voluntary DPIA should be treated as a useful tool to:

facilitate Data Controllers in the application of the principle of data protection by design and allowing them to anticipate potential impacts on the rights and freedoms of data subjects and implement stringent safeguards as soon as possible;
help national DPAs to assess the compliance of the processing and, in particular, the Risks for the protection of Personal Data of the Data Subject and the related safeguards;
complement, or to be a part of, a wider Risk management process a Data Controller has to implement and perform[11].

[7] See: The Recommendation 2012/148/EU

[8] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, revised and adopted on 4 October 2017.

[9] Article 35 (3) of the GDPR

[10] Article 35 (4) of the GDPR

[11] Indeed, although it is called an “assessment”, the DPIA goes beyond the simple analysis of Risks to data protection, by describing adopted or envisaged safeguards and measures in proportion to the Risks identified, thereby being based on a Risk management procedure rather than a mere risk assessment.

The Template, albeit itself non-compulsory, will serve the purpose as an evaluation and decision-making tool of supporting Data Controllers in the Smart Grids sector to comply with the legal requirements foreseen by Article 35 of the GDPR and voluntary commitments. The Template is also expected to contribute to coherent application of the relevant EU laws on data protection provisions across Member States and to promote a common methodology for Data Controllers guaranteeing adequate and harmonized processing of Personal Data.

The Template should help to ensure that Smart Metering System applications are monitored and that fundamental rights and freedoms of individuals are respected, by identifying data protection Risks in Smart Grid developments from the start. In this way, Data Controllers can take adequate measures in order to reduce these Risks and to mitigate the potential impact of the Risks on the Data Subjects, the Risk of non-compliance, legal actions and operational Risk. For that purpose, the Template defines the necessary process steps to find appropriate Controls attributed by examples of Controls measures. Last, but not least, Data Controllers in the Smart Grid environment that apply the Template may take competitive advantage by providing trust.

The Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems provided guidance to Member States on measures to be taken for the positive and wide-ranging dissemination, recognition and use of the Template.

Other benefits of applying the DPIA Template:

preventing costly adjustments in processes or system redesign by mitigating Risks to Privacy and Personal Data;
preventing discontinuation of a project by early understanding of the major Risks;
facilitating the compliance with the principle of minimisation and accuracy of Personal Data (quality of Personal Data);
raising awareness on Risks to Privacy and Data Protection within the organisation;
facilitating corporate decision-making on the basis of the DPIA report;
strengthening confidence of consumers, employees, citizens and DPAs by demonstrating compliance with the GDPR, respect to Privacy and commitment to safeguarding Personal Data protection;
stimulating public awareness or loss of credibility as a result of a perceived loss of Privacy or failure to meet expectations with regard to the protection of personal information.

Additionally, the execution of the DPIA will provide valuable information for different stakeholders within the Data Controller organization:

Investor / Management / Project Initiator / System Owner	Project Management / Change Management
Will the investment be feasible from the viewpoint of data protection?	Are non-functional and requirements sufficiently dealt with?
Are the Risks known and can they be mitigated?	Are the Risks known and are we (still) dealing with them?
Compliance and Oversight Functions	System Developers / Project Executions
Is the Risks Assessment properly executed?	What measures do we need to take?
Are all interests of stakeholders dealt with and balanced?	What are the boundaries for performing the work?

1.4. The Template Users – Smart Grid and Metering Systems' Operators

The following categories of entities may undertake the function of Smart Grid operators:

DSOs will be, or are already involved in the processing of Personal Data originated from Smart Grids or Smart Metering Systems. DSOs will have detailed information on the status of network components, generators connected to the network and energy flows throughout the network. This includes secure remote reading of Data Subject's metrological register(s) for all information needed for network management and quality of supply management. This information should be shared on an as needed basis to fulfil regulated duties with service providers like distributed generation operators and aggregators.

In most Member States one of the roles assigned to the DSOs is the one of the metering data hub where all the relevant Personal Data and non-Personal Data is stored and managed.

Generators: In a Smart Grid environment, it is expected that decentralised energy producers may need to have access to data consumption of neighbour consumer(s) to be able to supply the area islanded from the grid or to have better voltage quality by adjusting the production to the neighbouring consumptions.

Energy Suppliers will be involved in handling of billing data, management of debt, for preventing and detecting theft or fraud, providing energy efficiency advice measures services or other services based on consumption information of Data Subjects.

Metering Operators may act as companies, independent from DSOs or suppliers, responsible for reading meters, managing the metering infrastructure used by the Data Subjects, delivering Personal Data to other market actors (e.g. energy services companies, generators or alternative suppliers).

Energy Services Companies: Given the increasing variety of energy-related services (e.g. those offered by aggregators), the companies offering innovative services in the field of energy supply, demand response, aggregation, selling bundled etc. might need to access Personal Data of Data Subjects originating from Smart Grids in order to tailor and execute their services.

TSOs: Although, in theory, the TSOs could be Smart Grid operators qualifying as Data Controllers, in practice, current and envisioned models do not foresee that TSOs will be involved in the processing of Personal Data originated from Smart Grids or Smart Metering Systems.

1.5. Good Practices

The application of the DPIA Template may be strengthened and its output maximized with the adoption of a set of good practices.

The DPIA should:
be performed at an **early stage** (preferably during the design of new applications or systems);
involve **relevant** internal and external **stakeholders** in the process, including the data subjects – where appropriate;
be **future oriented** i.e. should support the identification of Risks to Privacy and Personal Data before the usage of new applications or implementation of new programs;
be **adjusted** during a project (especially when Risks to Privacy and Personal Data are changing);
be carried out by a **multidisciplinary team** of experts who have both knowledge of the project/program and access to relevant expertise concerning Privacy and Personal Data;
be subject to **formal or informal control process** performed by external/independent persons.

The DPIA should be a part of:
Risk management and/or has a structural place in projects, programs or processes;
a system of motivating, sanctioning and controlling;
the quality assurance process of a project methodology.

The DPIA should not be:
a tool for assessing the legal basis for the treatment of Personal Data;
an *ad-hoc* or random exercise;
used as a static document.

1.6. Terminology of the Template

1.6.1. Glossary

Actor	A logical component of Smart Grid or Smart Metering systems on which Personal Data can reside. [See more on Actors under Section 1.6.2]
Cardinality	Cardinality refers to the number of instances of an entity. For the purpose of DPIA, the Cardinality is a property of Actors (how many instances of that Actor are involved in the Use Case?) and of Personal Data (how many instances of a specific set of Personal Data reside on that Actor?).[See more on Cardinality under Section 1.6.2].
Control	Any measure or action that modifies Risk. Controls include any policy, procedure, practice, process, technology, technique, method, or device that modifies or manages Risk.
Cyber Security	All activities necessary to protect network and information systems, their users, and affected persons from cyber threats[12].
Data Controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data Processing	Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Processor	A natural or legal person, public authority, agency or other body which, alone or jointly with others, processes Personal Data on behalf of the Data Controller
DPA **Data Protection Authority**[13]	An independent public authority (-ies) which is established by a Member State responsible for monitoring the application of the EU Data Protection law in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of Personal Data within the EU.
DPO **Data Protection Officer**	A person with expert knowledge of Data Protection law and practices who advises the Data Controller or Data Processor with the EU Data Protection regulation and monitors internal compliance of the organization. Data Protection officers, whether or not they are an employee of the Data Controller, should be

[12] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act''), Art. 2.

[13] Defined as "supervisory authority" by the GDPR

	in a position to perform their duties and tasks in an independent manner.
DSO Distribution System Operator	A natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity; distribution system means the transport of electricity on high-voltage, medium-voltage and low-voltage distribution systems with a view to its delivery to customers, but does not include supply.
GDPR - General Data Protection Regulation	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1–88.
GDPR Requirements	Overall of the obligations stemming out of the GDPR, listed in Annex I
Level of Identification	An estimation of how easy it is to identify data subjects with the available data processed by the business process.
Likelihood	An estimation of the possibility for a risk to occur. It essentially depends on the level of exploitable vulnerabilities and on the level of capabilities of the risk sources to exploit them.
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Prejudicial Effect	An estimation of how much damage would be caused by all the potential impacts of a Threat with reference to the GDPR Requirements applied to each Primary Asset associated to the Threat.
Primary Asset	A set of one or more pieces of Personal Data allocated on a specific Actor i.e. on a logical component of the Smart Grid or Smart Metering project See more on Primary Assets under Section 1.7- DPIA Terminology].
Privacy	The right to be left alone and includes elements of protecting private life such as integrity of a person's home, body, conversations, data, honour and reputation pursuant to Article 7 of the Charter of Fundamental Rights of the European Union.
Residual Risk	A Risk that occurs after implementing a Risk Treatment option. It represents the remaining risk after applying one or more of the Risk management approaches.

Risk	A hypothetical scenario that describes the Likelihood that a potential Threat that affects directly or indirectly Personal Data has to occur, and the Severity of the impact that such Threat, if realized, would have on the rights and freedom of natural persons.
Risk Assessment	A process consisting of three steps/levels: (i) risk identification, (ii) risk analysis, and (iii) risk evaluation
Risk Source	A potential originator of Risks.
Risk Source Capability	An estimation of the capacity of Risk Sources to exploit vulnerabilities of Supporting Assets by keeping into account all factors that contribute to such capacity (skills, available time, financial resources, proximity to system, motivation, feeling of impunity, etc.).
Risk Treatment	A Risk modification process that involves selecting and implementing one or more treatment options. Once a Risk Treatment has been implemented, it becomes a Control or it modifies existing Controls.
Scenario	A possible sequence of interactions within a Use Case i.e. one of the possible routes in the description of a sequence of steps that compose a Use Case. A Scenario is described as a sequence of activity steps, each of them involving an activity performed by an Actor or other component, or an interaction between components [SG-CG/M490/E].
Severity	The Severity of a Risk is an estimation of the magnitude of potential impacts on the Data Subjects' Privacy. It essentially depends on the Level of Identification of the Personal Data and Prejudicial Effect of the potential impacts.
Smart Grid	An electricity network that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety.
Smart Metering System	An electronic system that can measure energy consumption, adding more information than a conventional meter, and can transmit and receive data using a form of electronic communication.
Supporting Asset	A physical component, upon which, an Actor – a logical component where Primary Assets (qualified sets of Personal Data) reside, is reliable.
Threat	An event / incident which could cause damage on Personal Data or the data subject.
Use Case	A specification of a set of actions performed by a system (for example an IT system that is involved in Smart Grid or Smart Metering System), which yields an observable result that is, typically, a value for one or more Actors or other component of the system. [SG-CG/M490/F]. A Use Case description includes primary Scenario of a Use Case that allows achieving the Use Case goal, and one

	or more alternative Scenarios covering different routes that may lead to achieving the goal or not [see Scenario definition above].
Vulnerability	The Vulnerability of a Supporting Asset is a weakness that can be exploited by one or more Threats.

1.6.2. Primary Assets, Supporting Assets and Actors

In the context of the Template and the Risk Management Methodology, qualified sets of Personal Data are referred to as "Primary Assets". A Primary Asset is a set of one or more pieces of Personal Data allocated on a specific Actor that shall be properly protected. It should be underlined that the same set of Personal Data may have different characteristics, be subject to different Threats, and may determine different Risk assessment metric values, depending on the Actor or Supporting Asset on which it is allocated[14].

E.g. consumption curves of a single customer allocated on a meter in the field and consumption curves of all customers allocated on the central system in cloud constitute different Primary Assets.

An Actor is an entity that communicates and interacts [*SG-CG/M490/E*] which can include people, software systems, field devices. For the purpose of the DPIA, Actors are ***logical*** components of the Smart Grid/Smart Metering solution under assessment on which Personal Data can reside.

E.g. An example of an Actor - logical component, is a Smart Metering central system this logical component has a number of associated Supporting Assets - underlying physical components, both software (applications, operating systems, databases) and hardware (machines, network appliances, etc.) , each of them exposed to different types of Data Protection and security Risks.

Actors rely on various ***physical*** components referred to as Supporting Assets. Supporting Assets can include the following:

Hardware: computers, communications relay, USB drives, hard drives, sensors, smart meters, Remote terminal units (RTU), intelligent electrical devices (IED), actuators, data concentrators, servers, front-ends, work stations, smart meters;
Software: operating systems, messaging, databases, business applications, Advanced metering infrastructure (AMI) Head-end;
Networks: electricity and data cable, wireless, fibre optic, routing and switching devices
People: users, administrators, top management;
Paper media: printing, photocopying, invoices, delivery contracts;
Paper transmission channels: mail, workflow diagrams, personalised web-portals.

[14] The Template refers to terminology adopted by the dedicated French public body - *Commission nationale de l'informatique et des libertés* (CNIL) in their Methodology for Privacy Risk Management. The CNIL Methodology for Privacy Risk Management can be found here: https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

Typically, for each Actor involved in the actions performed by the system within the Smart Grids' project (Use Case), Supporting Assets can be assigned to (one or more), while Primary Assets might be present or not.

E.g. For an Actor – a Smart Metering central system, the Primary Assets are the sets of Personal Data residing on the system (e.g. customer names and addresses, meter load profiles etc.).

For each Primary Asset the Supporting Assets are the underlying pieces of Hardware, Software, Networks on which each set of Personal Data reside.

One of the properties of Actors is their Cardinality. Cardinality refers to the number of instances of the Actor involved in the Use Case. Cardinality can also refer to Personal Data – the number of instances of a specific set of Personal Data residing on an Actor.

E.g. when analysing the process of load curves collection in a DSO that operates a low voltage network of 2M meters and 20k concentrators: the Cardinality of Actors is: 2M meters, 20k concentrators (each one managing 100 meters), 1 central system; the Cardinality of Personal Data (load curves) per Actor is: 1 for every meter; 100 for every concentrator; 2M in the central system. The Cardinality is an important property in the analysis of Risk: an attack compromising a single meter that hosts Personal Data for 1 customer is different than an attack compromising the central system that hosts Personal Data for 2M customers.

1.6.3. M490 Standardization Mandate

The Template contains a number of numerical references with a tag "**M490**". Those refer to standards adopted on the basis of M490 Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment.

1.7. Overview of the DPIA process

1.7.1. DPIA Step-by-Step

The following diagram provides an overview of the complete DPIA workflow. In the diagram, tasks in yellow are optional, and need to be performed or not depending on the outcome of preceding tasks.

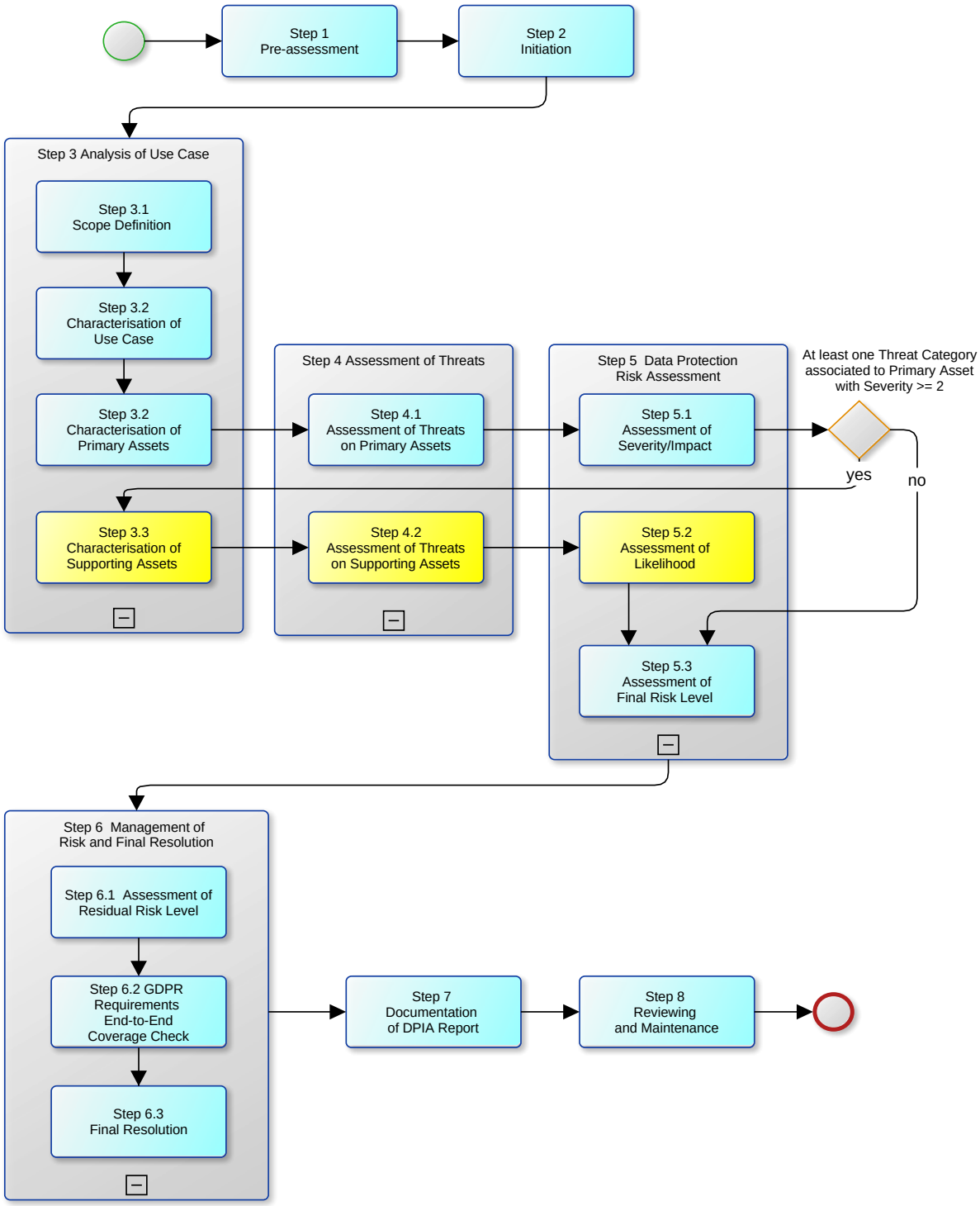


Figure 1. End-to-end view of DPIA workflow

Step 1 – Pre-assessment: In this step, the need whether or not to conduct the DPIA is evaluated based on a set of criteria. Outcome of this step is the decision to perform the DPIA, or not; in that case the DPIA process ends.

Step 2 – Initiation: In this step, the organisational work needed to prepare the DPIA is performed. This includes identifying and obtaining commitment for core and supporting members of the DPIA team, and identifying all necessary sources of information that will be used during the subsequent steps of the assessment.

Step 3 – Analysis of Use Case: Given the Smart Grid initiative, project or system(s) that may involve Personal Data to which the DPIA is targeted, purpose of this step is to determine the scope and boundaries of the DPIA assessment by providing a thorough representation of the processes and assets under analysis. This step can be broken down into four main tasks:

3.1 Scope definition: Purpose of this task is to provide a description of the Smart Grid Initiative targeted by the DPIA, determine the scope and boundaries of the assessment, and identify the Use Case involving Personal Data to be studied.
3.2 Characterization of Use Case: Purpose of this task is to provide a description of the Use Case(s) being analysed, of the Smart Grid components that realize them, and of the Use Case Scenarios where Personal Data are involved.
3.3 Characterization of Primary Assets: Purpose of this task is to analyze and characterize the Primary Assets involved in each described Scenario.
3.4 Characterization of Supporting Assets: This task must be performed only for Primary Assets affected by Threat Categories having a value of Severity resulting from task 5.1 with value >= 2, thus to focus the efforts on Primary Assets with Level of Identification or Prejudicial Effects that are, at least, both limited. Purpose of this task is to identify and describe the Supporting Assets (HW systems, SW systems, paper documents, field devices like meters, etc.) where Primary Assets reside.

Step 4 – Threat Identification: In this step, starting from the provided list of Threats clustered into Primary Asset Threat Categories and Supporting Asset Threat Categories, a list of Threat Categories applicable to the Use Case in scope is determined; then, for each Primary Asset Threat Category, affected Primary Assets are identified. Later on, in case Primary Assets with Severity >= 2 are determined, Supporting Assets are also identified and the relevant Supporting Asset Threat Categories are selected.

Step 5 –Risk Assessment: In this step, the Risk Level associated to each Threat Category identified in Step 4 is determined by applying a method split across three tasks:

5.1 – Assessment of Severity: In this task, Threat Categories identified in Step 4 affecting Primary Assets are evaluated according to two metrics:
Level of Identification of Personal Data established in the list of Primary Assets, i.e. how easy is to identify data subjects starting from the Primary Assets?
Prejudicial Effect of potential impacts of applicable Threat Categories, i.e. how much damage will be caused by the applicable threats should they become real?
Then, the two metrics are composed into a single value representing the overall Severity for each Threat Category.

-

5.2 – Assessment of Likelihood: This task must be performed only for those Threat Categories whose value of Severity/Impact resulting from the task above >= 2, otherwise it ca be skipped. In this task, Threat Categories identified in Step 4 affecting Supporting Assets are evaluated according to two metrics:
Supporting Assets Vulnerability, i.e. how easy it is to exploit the properties of Supporting Assets in order to carry out threats belonging to a certain Threat Category?
Risk Source Capability, i.e. given the sources that can originate threats (Insider, Outsider, Non-Human), how much capable are they to make the threat occur, accidentally or deliberately?
Then, the two metrics are composed into a single value representing the overall Likelihood for each Threat Category.

5.3 – Assessment of Final Risk Level: in this task, the Threat Categories are mapped on the Risk Quadrant and classified into five Priority levels based on their position in the quadrant.

Step 6 –Risk Treatment and Final Resolution: In this step, the Risks identified at Step 5 are treated using risk treatment techniques, then a final decision in taken by the Data Controller's management based on the Risk Treatment outcome. This step is split into three tasks:

6.1 Assessment of Residual Risk Level: This task represents the conclusion of the Threats and Risk Assessment method used within the DPIA. It includes:
Identification and assessment of implemented or planned controls in order to reduce the Risk.
Treatment of Risks, by determining which action (introduction of additional Controls, accepting the Risk as-is, etc.) to take to manage the Risk related to each Threat Category. The actions shall be taken to the assure compliance with the GDPR Requirements described in Annex I – and the controls listed in Annex II – List of Possible Controls.
Determination of the Residual Risk Level for each Threat Category i.e. the level of risk after the treatment has been applied, and mapping on the Threat Categories on the Residual Risk Quadrant.

6.2 GDPR Requirements' Coverage Checklist: In order to ensure that the Threat and Risk analysis has been done properly, a final check is done for verifying that for each Primary Asset, all applicable GDPR Requirements are satisfied.

6.3 Final Resolution: The final management decision is taken (e.g. based on cost/benefit analysis of Residual Risk Level, of planned Controls etc.) whether to consider the solution resulting from DPIA acceptable or not.

Step 7 – Documentation of DPIA Report: The main deliverable of the DPIA process is the DPIA Report. The report captures the work performed in each phase of the DPIA including the approved Final Resolution.

Step 8 – Reviewing and Maintenance: Purpose of this step is to ensure that the actions identified by the DPIA are actually carried out in the system(s) or project targeted by the DPIA process, and to assess the need to review the DPIA periodically or when new initiatives arise potentially involving Personal Data.

1.7.2. List of input and outputs

The following table summarises the inputs and outputs for each Step of the DPIA assessment. References to non-trivial input and outputs for each step is provided throughout the guidance part of the DPIA.

Table 1. Inputs and Outputs of each DPIA Step

Step	Input	Output
1		Decision whether or not to perform the DPIA > 2
2	1> Decision is DPIA must be performed	List of core DPIA team members and supporting DPIA team members List of Information Sources > 3.1
3.1	2 > List of DPIA team members 2 > List of Information Sources	List of Use Cases involving Personal Data > 3.2
3.2	3.1 > List of Use Cases involving Personal Data	Description of Use Case(s) > 3.3, 3.4
3.3	3.2 > Description of Use Case(s)	List of Primary Assets > 3.4, 4, 6.2
3.4	3.3 > List of Primary Assets 5.1 > List of Threat Categories affecting Primary Assets with Severity	List of Supporting Assets associated to each Primary Asset > 4
4	3.3 > List of Primary Assets 3.4 > List of Supporting Assets associated to each Primary Asset Annex III > Threats Taxonomy	List of Threat Categories affecting Primary Assets > 5.1, 5.2 List of Threat Categories affecting Supporting Assets > 5.2
5.1	4. > List of Threat Categories affecting Primary Assets Annex I > List of GDPR Requirements	List of Threat Categories affecting Primary Assets with Severity > 3.4, 5.2, 5.3, 6.1
5.2	5.1 > List of Threat Categories affecting Primary Assets with Severity 4 > List of Threat Categories affecting Primary Assets 4 > List of Threat Categories affecting Supporting Assets	List of Threat Categories affecting Primary Assets with Likelihood > 5.3 List of Threat Categories affecting Supporting Assets with Likelihood > 6.1
5.3	5.1 > List of Threat Categories affecting Primary Assets with Severity 5.2 > List of Threat Categories affecting Primary Assets with Likelihood	List of Threat Categories affecting Primary Assets with Final Risk Level and Priority > 6.1
6.1	5.1 > List of Threat Categories affecting Primary Assets with Severity	List of Threat Categories affecting Primary Assets with Residual Risk Level > 6.3

Step	Input	Output
	5.2 > List of Threat Categories affecting Supporting Assets with Likelihood 5.3 > List of Threat Categories affecting Primary Assets with Final Risk Level and Priority List of Personal Data Protection Targets (from DPIA Annex I) List of possible Controls (from DPIA Annex II)	
6.2	3.3 > List of Primary Assets List of Personal Data Protection Targets (from DPIA Annex I)	Personal Data Protection Targets coverage checklist > 6.3
6.3	6.1 > List of Threat Categories affecting Primary Assets with Residual Risk Level 6.2 > Personal Data Protection Targets coverage checklist	Final Resolution
7	Output from all preceding Steps	Signed Final DPIA Report
8	Signed Final DPIA Report	DPIA Review Report Recommendation on new DPIA

1.8. Disclaimer

The Template is the result of the consensus reached among experts of the Expert Group for Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment (EG2) within the Smart Grids Task Force.

The Template does not represent the opinion of the European Commission. Neither the European Commission, nor any person acting on the behalf of the European Commission, is responsible for the use that may be made of the information arising from this document.

2. Guidance for execution of the DPIA

This Chapter describes the steps to be taken when carrying out a DPIA. Furthermore, this Chapter can be read together with the questionnaire in Chapter 3.

2.1. Step 1 - Pre-assessment and criteria determining the need to conduct a DPIA

The GDPR requires the Data Controller to conduct a DPIA when the **type of processing** (collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction or other means) **is likely to result a high risk to the rights and freedoms of natural persons** - especially caused by using new technologies, and taking into account the nature, scope, context and purpose of the processing. The nature, scope, context and purposes can be determined by the data categories, by the purposes of the processing activities and by involving Data Processors.

Questions in section 3.1 are to facilitate the Smart Grids' operator to verify whether the criteria for carrying out a DPIA are fulfilled. Positive replies to those questions endorse the need to carry out a DPIA. This is not a quantitative exercise. This means that a single positive answer might make it necessary to conduct a DPIA. Therefore, this Chapter gives a recommendation how to interpret the DPIA criteria for grid-specific processes.

For this stage, assembling a wide DPIA team as described in point 2.2.2 is not compulsory since the scope and granularity of information needed to conduct the pre-assessment is not as wide as for the rest of the process. Nonetheless, the project leader and the Data Protection Officer shall be involved throughout the entire process.

Besides the below-mentioned criteria there could be other reasons or external influences that might lead to a need of performing a DPIA. These should be identified.

2.1.1. Criterion 1 – Cases foreseen by the GDPR, DPAs or European Data Protection Board

The **GDPR lists three particular case**s, for which, performing a DPIA is always required:

a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person
processing on a large scale of special categories of data referred to in Article 9(1) GDPR, or of Personal Data relating to criminal convictions and offences referred to in Article 10 GDPR; or
a systematic monitoring of a publicly accessible area on a large scale[15].

It should be noted that only the first case seems to be relevant for grid processing operations. When it comes to the second case, it should be underlined that special categories of Personal Data (Art. 9 and

[15] Article 35 (3) of the GDPR

10 GDPR) are typically not part of grid processing activities. Engagement of Smart Grid operators in monitoring of public areas is, as of now, not considered a business activity of Smart Grid operators.

The **general requirement coming from** the GDPR (DPIA in case of the type of processing which is likely to result a high risk to the rights and freedoms of natural persons) is subject to interpretation with regard to requirements of the GDPR as well as to working processes of relevant stakeholders, such Article 29 Working Party and the newly established EDPB.

Some indications come from the recitals and provisions of the GDPR, that might be relevant for Smart Grid operators, e.g.:

- recitals 71 and 91 classify **consumer evaluating or scoring**, including **profiling** and **predicting** as processing which is "likely to result in high risk";
- recital 91 mentioned Data Processing "**on a large scale**";
- article 22 and recital 91 mention "**preventing data subjects from exercising a right or using a service or a contract"**.

Additionally, the GDPR (art. 35.4) foresees an **obligation of the national DPAs** to establish lists of the kind of processing **operations requiring a DPIA** and, in the case where the processing is cross-border, the list of processing operations of the DPAs will go through the consistency mechanism[16].

The national DPAs are also allowed, on the basis of the GDPR (art.35.5) to adopt **lists** of the kind of processing operations for which **no data protection impact assessment is required**.

On 4 October 2017, the Article 29 Working Party adopted Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of the GDPR[17]. The Guidelines aim at clarifying this notion and providing criteria for the lists to be adopted by the national DPAs, as mentioned above.

The reference to the "**rights and freedoms" of data subjects** primarily concerns the rights to Data Protection and Privacy, but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion[18].

The reference to **likelihood of resulting "in a high risk to the rights and freedoms",** in turn, means that even if conditions triggering the obligation to carry out DPIA have not been met does not diminish Data Controller's obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects. In other words, **Data Controllers must continuously asses the risks** created by their processing activities in order to identify when a type of processing is "**likely to result in a high risk to the rights and freedoms of natural persons**"[19].

[16] Article 35 (4) of the GDPR
[17] Available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
[18] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, revised and adopted on 4 October 2017, p.6.
[19] Idem.

Please note that a new body called the European Data Protection Board (EDPB), regulated under Art.68-76 of the GDPR is to be established with the mission to issue guidelines, recommendations and best practices in order to encourage a consistent application of the GDPR. According to Article 29 Working Party (WP29), the EDPB is going to take on and expand the role of WP29 as the GDPR will become effective. The Board will issue guidance for Data Controllers and Data Processors – for example, on the data portability right, Data Protection Impact Assessments, certifications, and the role of Data Protection Officers. After becoming active, EDPB will be the premier source of information regarding the DPIA, including criteria about when the assessment should be performed.

In the future, it is possible that common European Union Lists of processing operations that are subject to the DPIA and for which the DPIA is not necessary[20].

It is also recommended, in cases **when it is not clear** whether a DPIA is required, the WP29 recommends to carry out a DPIA since it is a useful tool for Data Controllers to comply with the GDPR.

2.1.2. Criterion 2 - Relevant occurrence

In the case of the development of a new application or system, in compliance with the principle of Data Protection by design, a DPIA should be executed from the start of the idea throughout the design and implementation. This enables the Data Protection by design approach guaranteeing that potential Risks are identified and that appropriate Controls can then be built into the systems.

With already existing applications the following criteria should also be considered when envisaging a DPIA:

Significant changes in the Smart Grid application, such as material changes that expand beyond the original purposes (e.g., secondary purposes) or architectural changes (i.e. moving to cloud based services);
New types of information processed are introduced;
Unexpected Personal Data breach with significant impact and the occurrence of which hadn't been identified in the residual Risks of the application identified in the part 5 of the preceding DPIA;
The Data Controller in accordance with the Risk management policy might define periods of regular reviews of the DPIA report;
Responding to substantive or significant internal or external stakeholder feedback or inquiry;
In the context of change management procedures such as material changes that expand beyond the original purposes (e.g., secondary purposes): throughout the lifetime of the Smart Grid application, a new or revised DPIA Report would be warranted if there are technological-related changes in applications, etc. that may have data protection implications for the Smart Grid application under consideration.

Indicators demonstrating that adequacy or compliance of existing systems are not in line with latest standards or insights (e.g. systems that have not been built with Data Protection by design in mind) constitute as trigger elements for actualizing a preceding DPIA. Also material changes that would narrow the scope or minimize the collection or use of Personal Data shall be registered in the actualized DPIA, in order to keep an updated documentation of the Use Case.

[20] See: Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, revised and adopted on 4 October 2017, p.5.

2.1.3. Criterion 3 – Personal Data involved and DPIA – related Data Processing activities

Purpose of this section is to get an initial insight to the data collected and used to assess the potential necessity to execute a DPIA, in particular data relating to grid process activities. Personal Data is defined in the article 4 (1), of the GDPR[21]. Especially identification numbers and online identifiers are defined as Personal Data.

It is important to consider, anytime Personal Data is to be processed, whether it is absolutely necessary for operational purposes. If not, Personal Data Processing should be avoided whenever possible. A legal basis for Personal Data Processing must always be identified.

2.1.3.1. Examples of Personal Data

Specifically, for the Smart Grid applications, **non-exhaustive examples of Personal Data** which gives rise to conduct a DPIA, would be:
Consumer registration data: names and addresses of data subjects, etc.
Usage data (energy consumption, in particular household consumption, demand information and time stamps), as these provide insight in the daily life of the data subject
Amount of energy and power (e.g. kW) provided to grid (energy production), as they provide insight in the amount of available sustainable energy resources of the Data Subject
Profile of types of consumers, as they might influence how the consumer is approached;
Facility operations profile data (e.g. hours of use, how many occupants at what time and type of occupants)
Frequency of transmitting data (if bound to certain thresholds), as these might provide insight in the daily life of the data subject
Billing data and consumer's payment method

2.1.3.2. Examples of Data Processing

Additionally, for further guidance, consider **Smart Grid processes that typically require processing Personal Data**, thus, demanding the execution of a DPIA:
Remote readings for billing purposes
Frequent remote readings for network planning
Dynamic and advanced tariffing
Provide information to consumer online (e.g., Website, mobile App)
Remote switching.

2.1.3.3. Illustrative examples

E.g. 1: The utility makes a website available that allows the consumers to access their consumption data online. The consumers have to subscribe to this service and give their consent[22]. The Personal Data – by definition - has to be transmitted from the smart meter to the central systems in a secure way in order to mitigate to a satisfactory level the risk of a possible breach.

E.g. 2: Smart meters register consumption data every 15 minutes (configurable). The data concentrator collects this 15 minutes reading once a day and sends it back to the backend systems. These readings

[21] Additionally, further guidance regarding this definition can be found in the WP136 opinion of the Article 29 working Party on the concept of Personal Data

[22] A "consent" means any freely given, specific, informed and unambiguous indication of the data subject's (natural person/ an individual) wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her (art. 4).

might be considered private information in such a way that they can be illegitimately used to assess sensitive information regarding the behaviour of each client.

E.g. 3: Implementing Smart Charging of EVs, calls for an interaction and corresponding information exchange between DSOs, Charge Spots, EVs, EV drivers and new market participants. To the latter, one could count a Charge Service Provider (CSP) which deals with fulfilling the charge wish of the EV driver and a Charge Spot Operator (CSO), which deals with the operation of the Charge Spots. Without measures, one could derive the charge locations of an EV throughout time. If this could be coupled to an EV driver, it would then become Personal Data as it reveals the whereabouts of the latter. Without taking into account the Data Protection concerns, this might lead to a lower acceptance of EV, and Smart Charging.

E.g. 4: The advanced Smart Grid functionality of load balancing requires data collectors to have near real time access to the mapped meters readings to be able to efficiently manage energy production and consumption, including micro generation and distributed generation. The Smart Meter readings are critical for the processing of the Smart Grid response for a load balancing event using the described strategy of near real time data collection on meter level.

2.1.3.4. Examples related to remote reading

Relating to the case of **remote readings** for billing purposes, the following non-exhaustive list below provides some illustrative examples of processing operations involving Personal Data:
Reading out a meter manual/remote, entering data into database
Storage of meter data in meter or telecommunication device incl. intermediate storage
Adding meter data to tariff registers in the meter and/or back end systems,
Transmission of meter data / tariff register data via WAN to a back end system naming addressing, encryption, data plausibility mechanism (e.g. detecting tampered data)
Applying tariffs to the meter data, e.g. multiplication of annual consumption with price/kWh in the back end system
Creating a bill out of the aforementioned data (Billing data)

2.1.3.5. Examples of non-Personal Data used in Smart Grid or Smart Metering processes

Locally produced weather forecast – consumption prediction / forecasts;
Demand forecast of building, campus and organisation;
At non-private feeder, transformer or network level (no link to individual consumers and their behavior. Consumption, frequency, voltage etc.).
An energy supplier maintains a list of systems and versions provided (e.g. leased) to a micro grid operator. This data will not be considered as Personal Data.
Technical data and commercial information are stored and processed in different systems. The common key (also called primary key) that is used to link the two types of data is location (the address). This way, client's Personal Data is better protected as it is not directly available when accessing technical data only

2.1.4. Criterion 4 – Status of a Data Controller or a Data Processor

The Smart Grid operators need to clarify if they can be considered as a Data Controllers. If the operator, alone or jointly with others, **determines the purposes, conditions and means** of operating Smart Grid applications or systems which has impacts on Personal Data, it is role is the of the Data Controller according to the GDPR.

Alternatively, the Smart Grid operator should determine if it fulfils the role of a Data Processor i.e. if it **conducts the identified processing operations on behalf of the Data Controller**. In other words, if the mere processing lies with the Smart Grids operator while another entity is a Data Controller i.e. determines the purposes, conditions and means. It might then suggest to the Data Controller to conduct a DPIA and assist them for this task within the limit of its responsibility. These two roles are defined by Article 4 of the GDPR[23].

In most EU Member States Smart Grid operators are DSOs. DSOs are then Data Controllers for the first part of the metering data process (DSO´s process ends with creating a bill for network usage; in a second step the metering data is being passed on to the supplier who will create a bill for the electricity supplied). DSOs can outsource parts of their metering business to a Data Processor (e.g. reading out meters, delivery of meter data to a DSO). In this case, the outsourcing partner/Data Processor has to assist the Data Controller with appropriate information so that the Data Controller can conduct the DPIA.

E.g.1: An energy supplier and an insurance company work together to provide insurance that covers stability of energy supply for micro-grid operators. In order to assess applicability of coverage, monitoring in energy supply is implemented. The respective role and responsibilities of all parties involved needs to be made clear.

It is also worth analysing whether it is feasible to carry-out a single DPIA by multiple Data Controllers. In accordance with The Article 29 Working Party guidelines on the DPIA such situation might take place where a similar technology is used to collect the same sort of data for the same purposes. Additionally, a DPIA can be also useful for assessing the data protection impact of a technology product:

E.g.2. A piece of hardware or software which is likely to be used by different Data Controllers to carry out different processing operations; In such case the Data Controller deploying the product (e.g. utility) remains obliged to carry out its own DPIA with regard to the specific implementation, but this can informed by a DPIA prepared by the product provider (smart meters' manufacturer), if appropriate. Each product provider should share useful information without neither compromising secrets nor leading to security risks by disclosing vulnerabilities[24].

2.1.5. Criterion 5 - New technologies and other criteria

If a decision of the Data Controller or Processor leads to an implementation of new technologies, a DPIA has to be conducted – especially if one of the above criteria already provides an indication for a need to perform DPIA[25].

New technologies within grid processes could be:

- smart meter environment;
- cloud processing;
- Internet of things.

[23] Further guidance can be found in the WP 169 opinion of the Article 29 Working Party *on the concepts of Data Controller and Data Processor*.
[24] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, revised and adopted on 4 October 2017, p.7-8.
[25] See also: recitals 89 and 91 of the GDPR.

2.1.6. Documented Conclusion

At the end of this section, a documented conclusion should be produced based upon the answers to the questions. This should be endorsed by the management regarding whether a DPIA is needed or not.

Output > Step 2
Documented decision endorsed by higher management on whether or not the organisation shall conduct a DPIA

2.2. Step 2 - Initiation

Before describing the process itself, the Template presents a non-exhaustive series of organisational guidelines which will contribute to the success of the DPIA. The table in section 3.2 should help by documenting necessary information.

2.2.1. Internal organisation

Three possible options for the management of the DPIA should be envisaged, each of them has its merits and drawbacks. **When the resources of the organisation allow it, option 1 should be favoured.**

Option I: A **dedicated team** within the organisation, but not the one in charge of the Smart Grids or Smart Metering application: - employees with knowledge of the automation environment (hardware, software, networks and network components); - employees in the user environment; - the Data Protection Officer could be involved as advisor to this team from an independent role.
Option II: a **third party** providing an external expertise needed for the DPIA
Option III: the **persons in charge of the application/system** which is the target of the DPIA. This might especially apply in the case of SME's with limited resources.

A key success factor for the success of the DPIA is the support of higher management. If higher management does not give the necessary support, the workload and time could be increased and the results can be disputed or disregarded.

2.2.2. The DPIA team

Under option 1, the team conducting the DPIA should be as independent as possible from the team working on the Smart Grid application itself. Becoming a member of this team requires strong understanding of the project itself, knowledge of Privacy, Data Protection and Cyber Security and expertise in the performance of risk assessments generally and privacy impact assessment in particular. Because of the diversity of expertise and interests involved, it is common to conduct the DPIA with a small and multidisciplinary team:

Team Members' responsibilities	
Project management	Legal
Risk assessment	Information and Cyber Security
IT architecture and system engineering	Organizational design
Privacy and Data Protection	Knowledge of the relevant business process
Roles	
DPIA Project Leader	Personal Data Protection Expert
Smart Grids System Architect	Information Security Officer
Smart Grids Operations Expert	Legal and compliance officer
Advisor on the Business Process	
Optional Roles	
IT Network engineer	
IT Cybersecurity Operations expert	
IT Service management	

2.2.3. The Sources

The necessary sources that will be used to execute the DPIA will be obtained by interviews or available in documents such as:

Project documents such as Project plan, Project initiation document, business case
Architectures, such as IT and Enterprise architectures
Requirements documentation, such as functional, technical and non-functional requirements
Type of data to be generated and its purpose of use
Contracts with system engineers, IT hosting parties, IT service providers, Installation and service providers
System design documentation, such as interface design, communication protocols
International Standards and Technical Reports on which the DPIA methodology relies. Acquaintance with the following documents is suggested for a better understanding of Step 3: • *SG-CG/M490/B_ Smart Grid First set of standards* • *SG-CG/M490/C_ Smart Grid Reference Architecture* • *SG-CG/M490/E_ Smart Grid Use Case Management Process* • *SG-CG/M490/K_ SGAM usage and examples*[26] • *IEC 62559-2:2015 Use case methodology - Part 2: Definition of the templates for Use Cases, Actor list and requirements list*[27]

While documenting the various sources of information useful for the DPIA process, there should be an indication of their specific purpose and in which steps they are used. The result of obtaining this information will be a good understanding and description of the data flow and the parties and systems involved in that data-flow as well as the Data Protection and security measures envisaged.

Output > Step 3.1
List of DPIA team members **List of information sources**

[26] Available at http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids

[27] Available through IEC webstore (https://webstore.iec.ch/publication/22349)

2.3. Step 3 – Analysis of Use Case

The objective of this Step is to define the scope and boundaries of the DPIA and to provide a comprehensive description of the Primary Assets and the Supporting Assets in scope of the DPIA. In this Step, the Data Controller should gather detailed information about the use of Personal Data in the business processes and underlying IT/OT technologies that are involved in the Smart Grid project under assessment. The List of Information Sources identified during Step 2 will provide necessary information for the analysis of each Use Case.

This Step of the DPIA is a very critical activity since it is where all the knowledge needed for the subsequent steps is gathered. Collecting such knowledge using a standard, internationally accepted methodology allows producing more comparable results, so that stakeholders reviewing multiple DPIA Reports released by different teams/organisations do not have to analyse the methodology but can focus on deliverables.

The suggested approach for the Analysis of the Use Cases relies on:

- The methodology described in M/490 CEN-CENELEC-ETSI Smart Grid Coordination Group set of reports[28];
- The Use Case Template described in IEC international standard, *IEC 62559-2:2015 Use case methodology - Part 2: Definition of the templates for Use Cases, Actor list and requirements list*[29].

The Template encourages DPIA teams to adopt the method proposed in this section, but organisations that have a well-structured Use Case analysis methodology in place may leverage on their own methods. In the latter case, the assessment team must ensure that the output of the analysis (Description of Primary Assets and Description of Supporting Assets) includes the same information and the same level of detail as the DPIA Template method. This Step is structured as follows:

1. The scope and boundaries of the Smart Grid project targeted by the DPIA are identified, then, among the Use Cases in scope for the project, the ones involving Personal Data are selected.
2. For each Use Case: • involved Actors are identified, then the Use Case is mapped as diagrams using SGCG Smart Grid Architecture Model (SGAM). • Scenarios (flows of execution within the Use Case) involving Personal Data are identified and described step-by-step.
3. For each Scenario step, Primary Assets are identified.
4. Identified Primary Assets are described based on a set of criteria
5. For each Primary Asset Supporting Assets are identified and described based on a set of criteria.

[28] Available at http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids
[29] Available through IEC webstore (https://webstore.iec.ch/publication/22349)

The workflow of tasks for Step 3 is represented in the following diagram. The next sections will provide detailed information about how to complete each task.

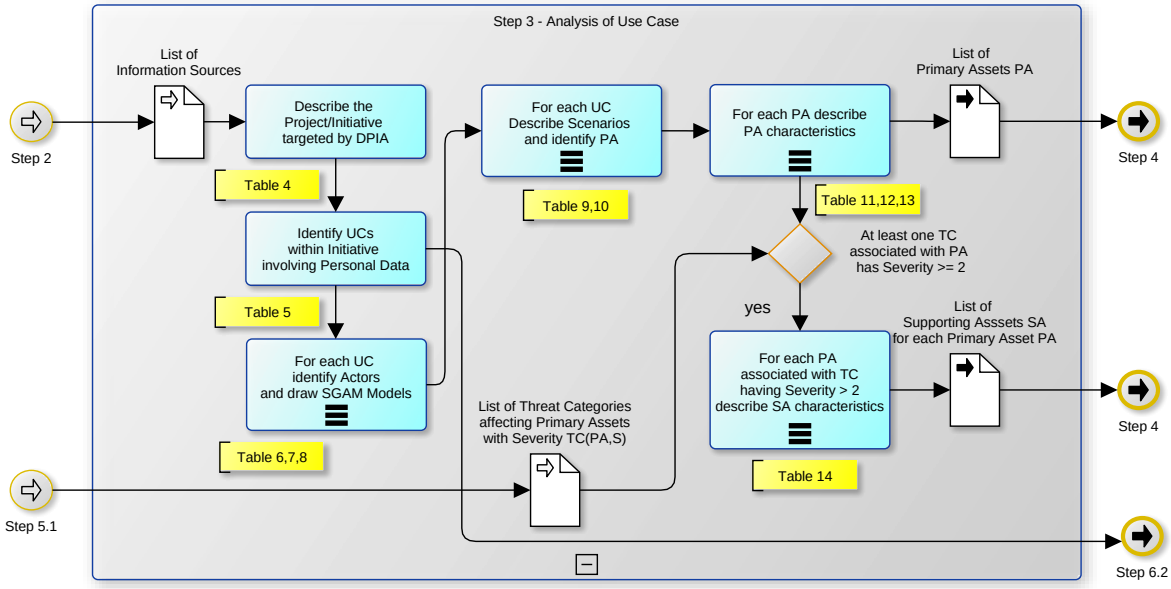


Figure 2. Workflow of Step 3 – Use Case Assessment

2.3.1. Scope definition

The first task to perform for the Analysis of the Use Case is to provide a description of the Smart Grid project targeted by the DPIA. This project might be a Smart Grid-related initiative, change request, or system(s) within the organization that involves Personal Data Processing.

The description can be in narrative form; in order to be helpful in the subsequent tasks of Step 3, it should clarify the boundaries of the analysis, specifying what is in scope for the initiative. The description of the initiative can be provided using Table 4: *Description of the target initiative of DPIA* under 3.3.1.

Once the scope and boundaries of the Smart Grid project, within which the DPIA is being performed, have been clarified, the portions of Smart Grid processes included in such boundaries are described by identifying the **Use Cases** supported by the project. Use Cases can be analysed at different scopes and at different levels of abstraction. A classification and definition of different types of Use Cases is provided in [*SG-CG/M490/E_Smart Grid Use Case Management Process* section 6.5.3 *Use case structure / definitions of different Use Cases types*. When performing the analysis for Step 3, the following concepts are useful:

Classification based on level of granularity and abstraction: Generic Use Case (GUC) vs Individual Use Case (IUC)
GUC - Use Cases are called generic when their description is broadly accepted in standardization and not project or technology specific.
IUC – In real projects, a company might develop company-specific Use Cases by evolving or combining GUCs

Classification based on applicability in regional or business context: High-Leve Use Case (HL-UC) vs Primary Use Case (PUC)
HL-UC: Describes the general idea of a function together with generic actors. The HL-UC can be realized in different ways, so the HL-UC cannot be mapped to a specific system or architecture.
PUC: A Use Case implemented in a specific system characterized by a defined boundary (it can be mapped on a defined architecture). The Use Cases can be mapped to a proposed architecture (SGAM).

For the purpose of the DPIA, in order to identify Primary Assets and Supporting Assets, Use Cases need to be mapped for the specific organization architecture so that actual Actors, communication channels and underlying IT and OT technologies can be identified. For this reason, the suggested level of detail should be the one of Primary Use Cases set to the same scope as the Smart Grids project itself, with the following level of abstraction:

- The Primary Use Case can be mapped on SGAM Component Layer (see section 2.3.2.3) i.e. Actors must be represented as systems and devices, not generic business roles;
- The Primary Use Case can be mapped on SGAM Communication Layer (see section 2.3.2.3) i.e. the Communication Channels used by Actors and related technologies/standards for communicating must be included in the Use Cases analysis.

A starting point for identifying Use Cases applicable to the Smart Grid project targeted by the DPIA is provided by *SG-CG/M490/B_ Smart Grid First set of standards* document. Section 7.5.1: *List of Generic Use cases* contains a list of Generic Use Cases that are broadly accepted as covering several Smart Grid processes. Then, for each domain of the Smart Grid, section 8 *Per systems standards mapping* provides a list of High Level Use Cases.

Starting from the lists provided by *SG-CG/M490/B*, the list of Primary Use Cases in scope for the target Initiative can be derived; *SG-CG/M490/E_Smart Grid Use Case Management Process* sections 9.2.1 and 9.2.2 give some examples of Primary Use Cases associated with High Level Use Cases. Finally, within the list of in-scope Primary Use Cases, the ones potentially involving Personal Data need to be checked.

Table 3.2.1.2 *List of Use Cases supported by the target initiative* shall be used to provide information about the list of Use Cases involving Personal Data. It will also be used in the final end-to-end check of coverage of GDPR Requirements.

Output > Step 3.2
List of Use Cases involving Personal Data

2.3.2. Characterisation of Use Case

Purpose of this section of the DPIA assessment is to provide a comprehensive description of the Use Cases involving Personal Data. The proposed approach is based on M/490 SGCG Reports and IEC 62559-2:2015 Standard. *SG-CG/M490/K_ SGAM usage and examples* which is an excellent source of information and samples for describing and modelling Use Cases according to this methodology.

If the Smart Grid operator has its own methodology and deliverables for Use Cases analysis, they can be used. In such case, the methodology needs to be referenced and attached to the DPIA report replacing this section, provided they contain all the information needed for describing Primary Assets and Supporting Assets in the subsequent tasks of Step 3. This task must be performed for every Use Case in scope involving Personal Data.

2.3.2.1. Description of Use Case

The first task for Use Case analysis it to provide a short description of the Use Case. Aside giving a short narrative overview of the Use Case primary scenario, the description should answer to the following questions:

- Does the description define domains & zones of SGAM?
- Does the Use Case description define the scope and systems boundaries?
- Which legal requirements must be considered?

Table 3.2.2.1: Description of Use Case can be used to collect the needed information.

2.3.2.2. Description of Actors

The second task in Use Case analysis is to identify and describe Actors. According to the definition in in SG-CG/M490/E[30], Actors can be:

- External: entity having behaviour and interacting with the system under discussion (system as "black box") to achieve a specific goal;
- Internal: entity acting within the system under discussion (Actor within the system; system as "white box") to achieve a specific goal.

According to such definition, within SGCG methodology Actors represent any component that participate in the Use Cases; as such, an Actor is where Personal Data reside and where Personal Data Processing operations occur.

As for Use Cases, Actors can be studied at different levels of abstraction. For the purpose of the DPIA, Actors must be represented as roles, systems, devices that can be mapped on the SGAM Component and Communication Layers (see section 2.3.3.3). Actor Types can be:

System - if referring to a device/appliance or OT component
Application - if referring to a SW application or IT component
Role - if referring to an individual
Organization - if referring to an entire organization; this type usually refers to external Actors

Table 3.2.2.2: *Description of Actors* can be used to collect the needed information.

[30] *Annex A* of the same document provides a comprehensive list of standardized Smart Grid Actors with description.

2.3.2.3. Representation of Use Case on SGAM Layers (Diagrams)

In order to provide a standardized view of the Use Case, to allow the comparison between Use Cases and to help determine the characteristics of Primary Assets and Supporting Assets in the subsequent tasks of Step 3, the suggested approach is to provide a representation of the Use Case using the SGAM Framework.

The **SGAM Framework** is a three-dimensional model of the Smart Grid composed of:

I. A **Smart Grid Plane** i.e. a matrix made of
Domains (Bulk Generation, Transmission, Distribution, Distributed Energy Resources –DER–, Customer Premises), the represent the domains of the electrical energy conversion chain;
Zones (Process, Field, Station, Operation, Enterprise, Market), that represent the hierarchical levels of power system management.
II. A set of **Interoperability Layers** (Business, Function, Information, Communication, Component),
Each of them provides a view of the entire Smart Grid Plane with a specific level of abstraction and with specific objectives.

Figure 3 provides an overview of how Domains, Zones and Interoperability Layers concur in building the SGAM Framework. For a detailed explanation of SGAM Framework, please refer *to SG-CG/M490/C_ Smart Grid Reference Architecture* Section 7.2 *SGAM Framework Elements*.

For the purpose of this Step, it is requested to map the identified Actors and their collaborations:

On the *SGAM Component Layer*: For instructions about how to draw the diagram please refer to document *SG-CG/M490/B_ Smart Grid First set of standards* section *7.4.3 – Conventions used to draw the component layer of a system mapping*. For an example related to Smart Metering, see in the same document Figure 37 - *Smart Metering architecture (example) mapped to the SGAM component layer.*

On the *SGAM Communication Layer*: For instructions about how to draw the diagram please refer to document *SG-CG/M490/B_ Smart Grid First set of standards* section 7.4.3 – Conventions used to draw the communication layer of a system mapping. For an example related to Smart Metering, see in the same document Figure 38 - *Smart Metering architecture (example) mapped to the SGAM communication layer*

The following table *Representation of Use Case on SGAM Interoperability Layers* provides empty Smart Grid Planes that can be used to draw the requested diagrams.

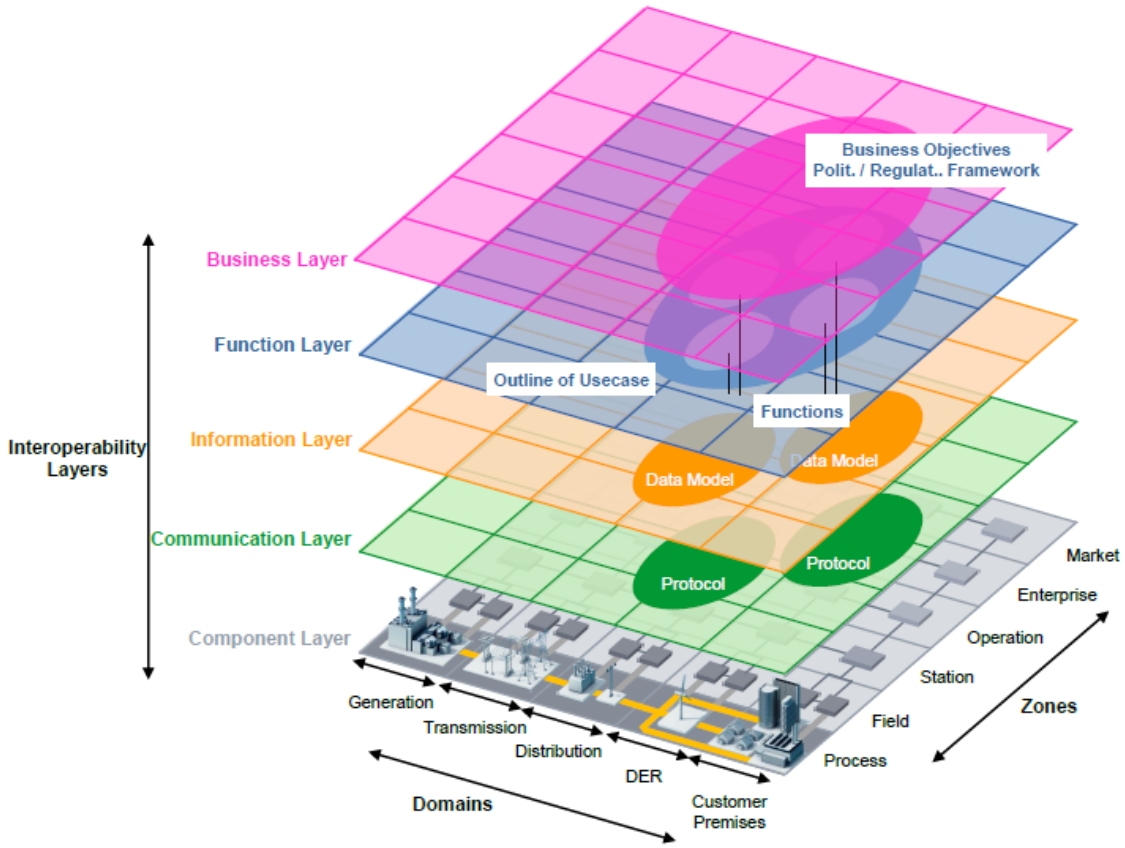


Figure 3. SGAM Framework

2.3.2.4. Description of Scenarios (step-by-step analysis of Use Case)

The last task of Use Case description is about identifying and analysing Use Case Scenarios. Usually, at least the primary scenario of each Use Case should be described; other scenarios may be needed if they involve different Actors, or if they affect different pieces of Personal Data or different Data Processing operations.

First, Scenarios involving Personal Data for this Use Case need to be listed using Table *List of Use Case Scenarios involving Personal Data*, identifying the Primary Actor that is the Actor that triggers the Scenario. Then, for each identified Scenario, a step-by-step analysis must be performed compiling Table: *Step-by-step description of Scenario related to Personal Data*. This analysis consists in identifying and describing the sequence of Activity Steps that compose the Scenario, providing the following information:

- *Information Producer* and *Information Receiver*: these must belong to the list of Actors identified at Section 2.3.3.2. If the step is an exchange of information, these are the source and recipient of information exchanged, if the step is a processing of information inside an Actor, then the Producer and Receiver coincide with that Actor.

- *Personal Data involved*, and *Data Processing operation performed*: this is where the Primary Assets involved in the Use Case are identified.

Output > Step 3.3, 3.4
Description of Use Cases

2.3.3. Characterisation of Primary Assets

The **Personal Data when allocated to specific Actors identified during the analysis of Scenarios are the Primary Assets of the DPIA**. The identification and description of Primary Assets is the main output of Step 3 of the DPIA.

Please note that certain operations that create association of Personal Data may be decisive on the Primary Asset status. For example, fully anonymized meter consumption data (Non-Personal Data) are different from consumption data associated to customer name (Personal Data). While performing the analysis of the Primary Assets, the following questions should be addressed:

On Actors:
On which Actor do the Primary Assets reside?
Where is the Actor located on the Smart Grid Plane? E.g. data residing in the field vs data hosted in a company Data Centre are exposed to different Threats
How many instances of the Actor exist (Cardinality of Actor)? E.g. data residing on millions of meters vs data residing on a single centralized System
How many data subjects for that Personal Data reside in each Actor instance (Cardinality of Personal Data per Actor). E.g. one meter hosting data for a single customer vs central system hosting data for all customers

On Personal Data:
I. Category: Which category does the data belong to? (Please note that if an Actor only contains non-Personal Data, data that are placed within this Actor do not qualify as a Primary Assets.)
Special categories of Personal Data as defined in Art. 9 GDPR or Personal Data relating to **criminal convictions and offences** as defined in Art. 10 GDPR, such as: - racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; - processing of genetic data, biometric data for the purpose of uniquely identifying a natural person; - data concerning health or data concerning a natural person's sex life or sexual orientation.
Personal Data in the context of grid environment, the processing of which might possible - impact the rights and freedoms of natural persons, such as: - personal identifiable consumption data; - bank account data (e.g. of natural persons running a photovoltaic systems or other renewable power plants); - grid use data personally related (voltage, electric current, phase angel); - geolocation data.
Non-Personal Data, such as: -anonymized consumption data; -technical meter data, such as voltage curve at the meter
II. Data Subjects: Which Data Subjects are affected?
III. Retention Time: How frequently are Personal Data accessed and how long are they kept within the Actor?

On **Data Processing operations**, the fundamental question than embeds the spirit of the GDPR is: **does the Data Processing may result in the risks to the rights and freedoms of data subjects?**

On Personal Data Processing operations :
Which processing operations (including exchange of data between Actors) of Personal Data are concerned with this Primary Asset? (This can be answered providing reference to the Scenario and Step).
Which are the purposes of the processing? (If applicable) Is there a legitimate interest pursued by the Data Controller that justifies the processing?
What is the degree of necessity of the processing operation in relation to the purposes?
Are there legal obligations for the processing operation?
Who is the Data Controller?
Who is the Processor?
Cardinality of Personal Data per Actor: How many Data Subjects for that Personal Data reside in each Actor instance e.g. one meter hosting data for a single customer vs central system hosting data for all customers

When assessing Personal Data Processing operations in Scenarios where multiple parties are involved (e.g. DSO metering data transmitted using Telco carrier public network, then stored on IT infrastructure belonging to a cloud Service Provider), it is of great importance to identify all parties involved and to determine which parties hold the role of Data Controller and which hold the role of Data Processor as the GDPR provides for different obligations for Data Controllers and Data Processors.

Table *Description of Primary Assets*, composed of Table *Actor, Personal Data* and *Processing Operation*, can be used to gather the information related to Primary Assets by filling one row for each Primary Asset (i.e. a Personal Data residing on a specific Actor) identified during the analysis of Scenarios of all Use Cases in scope involving Personal Data. It is important to remark that the same Personal Data residing on different Actors represents different Primary Assets, so the same Personal Data residing on different Actors results in multiple rows in the Primary Assets table.

For each Primary Asset a separate row must be filled in the Tables.

Output > Step 3.4, Step 4, Step 6.2
List of Primary Assets

2.3.4. Characterisation of Supporting Assets

Step 3.3 > Input
List of Primary Assets
Step 5.1 > Input
List of Threat Categories with associated Primary Assets and Severity

Primary Assets represent Personal Data allocated on Actors i.e. on *logical* components, that can be identified as part of an analysis performed at business process level. These Primary Assets however reside on and are realised by *physical* IT or OT systems or components, or communication channels that are named **Supporting Assets**.

Unlike Primary Assets, the analysis of Supporting Assets is done at IT and OT architecture, infrastructure, and/or application level and usually requires involvement of different skills and resources compared to the tasks performed in the rest of Step 3.

The analysis of Supporting Assets is the second output of step 3 of DPIA and is needed for every Primary Asset associated to at least one Threat Category having a Severity value >= 2 resulting from Step 5.1, thus requiring Likelihood Assessment: as a prerequisite of Likelihood Assessment, Supporting Assets need to be analysed.

The following questions should help in providing a useful characterisation of Supporting Assets:

On IT and/or OT resources that underlie the Primary Asset:
Which kind of hardware (computers, routers, electronic media, etc.)?
Which kind of software (operating systems, messaging systems, databases, business applications, etc.)?
What are the kind of computer communications networks (cables, Wi-Fi, fibre optics, etc.)?
On human resources involved:
Which roles are involved in accessing or processing the Primary Asset?
Which human tasks are performed related to the Primary Asset?
Which AAA (authentication, authorisation, accounting) [31] mechanisms are used to enforce Personal Data access rights?
On paper resources involved with the Primary Asset:
Which kind of supporting paper media (printouts, photocopies, etc.)?
Which paper transmission channels (mail, workflow, etc.)?

In order to select the proper level of detail of the analysis of Supporting Assets, the Data Controller should keep in mind that Supporting Assets will be used in Likelihood Assessment i.e. they will be assessed in terms of how easy it will be to exploit their weaknesses.

Table *Description of Supporting Assets* shall be used to gather the information related to Supporting Assets by filling one row for each Primary Assets for which the Likelihood Analysis is needed.

Output > Step 4
List of Supporting Assets (SA) with description.

[31] Set of IT mechanisms used to enforce user access rights to a resource. Authentication refers to identify the user (e.g. with user name and password); Authorisation refers to which permissions are given to the identified user; Accounting refers to tracking the user activity

2.4. Step 4 – Threat Identification

Step 3.3 > Input
List of Primary Assets
Step 3.3 > Input
List of Supporting Assets associated to each Primary Asset
Annex III > Input
Threats Taxonomy

Risks to rights and freedoms of individuals are mainly consequences of Threats affecting Primary or Supporting Assets in a way that might trigger an adverse event. The goal of this step is to identify the Threats to Data Processing. ENISA Threat Taxonomy[32] and its categories as well as specific highlights regarding personal Data Protection[33] have been adopted as a reference in the Template in order to ease the evaluation of the Threats to Primary or Supporting assets. Another input that is used during the Threat Identification is the list of **Risk Sources**.

Risk Sources - types of potential **originators of Risks**- are classified according to the following list:
Insider: persons who belongs to the organisation: user, system operator, grid operator, service operator, call centre operator, commercial service employee
Outsider: persons from outside the organisation: recipient, provider, competitor, authorized third party, government organisation, human activity surrounding, external/sub-contracted maintenance
Unintentional: corrupt sensor, natural disaster such as lightning, energy imbalance, energy disruption an outage.

The methodology first assesses the Severity of a selection of Threats affecting Primary Assets. Then, a second assessment is run only for those Supporting Assets that are related to Primary Assets classified as "High Impact Primary Assets" based on the analysis performed under Step 5.1 (through evaluation of Severity of the related Threats).

Examples of Threats that may affect the rights and freedoms of the data subjects and that need to be properly and systematically assessed and ultimately mitigated:
Impossibility to execute their rights by Data Subjects: right to information, correction or deletion of data, due to inexistence or damage to databases
Change in Data Processing: it deviates from what was originally planned (diversion of the purpose, excessive or unfair collection...)
Illegitimate access to Personal Data: it is known by unauthorized persons
Unwanted change in Personal Data: it is altered or changed
Disappearance of Personal Data: it is not or no longer available
Diverting of Personal Data to other users: it is distributed to people that do not need the access to it

[32] ENISA Threat Taxonomy, version 1.0, 2015, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

[33] See recital 75 of the GDPR

Whenever available within the organisation, the Data Protection Officer should take part to this analysis as an advisor as already suggested in section 2.2.2.

Starting from the analysis performed in Step 3 (Use Case Analysis), for each Threat Category it is required to identify the relevant Primary Assets and Risk Sources. The aim is to establish, for the Use Case(s) under the scope of this assessment, **a detailed and prioritized list of all Threats that** would trigger Risks and to provide information to evaluate the Severity of these Threats on the Primary Assets.

If a Primary Asset will be identified having at least one associated Threat Category with a Severity value >= 2, the related Supporting Assets need to be considered and a drill down on Supporting Asset Threats must be executed.

Figure 4 shows the workflow for this Step and its relationship with the rest of DPIA.

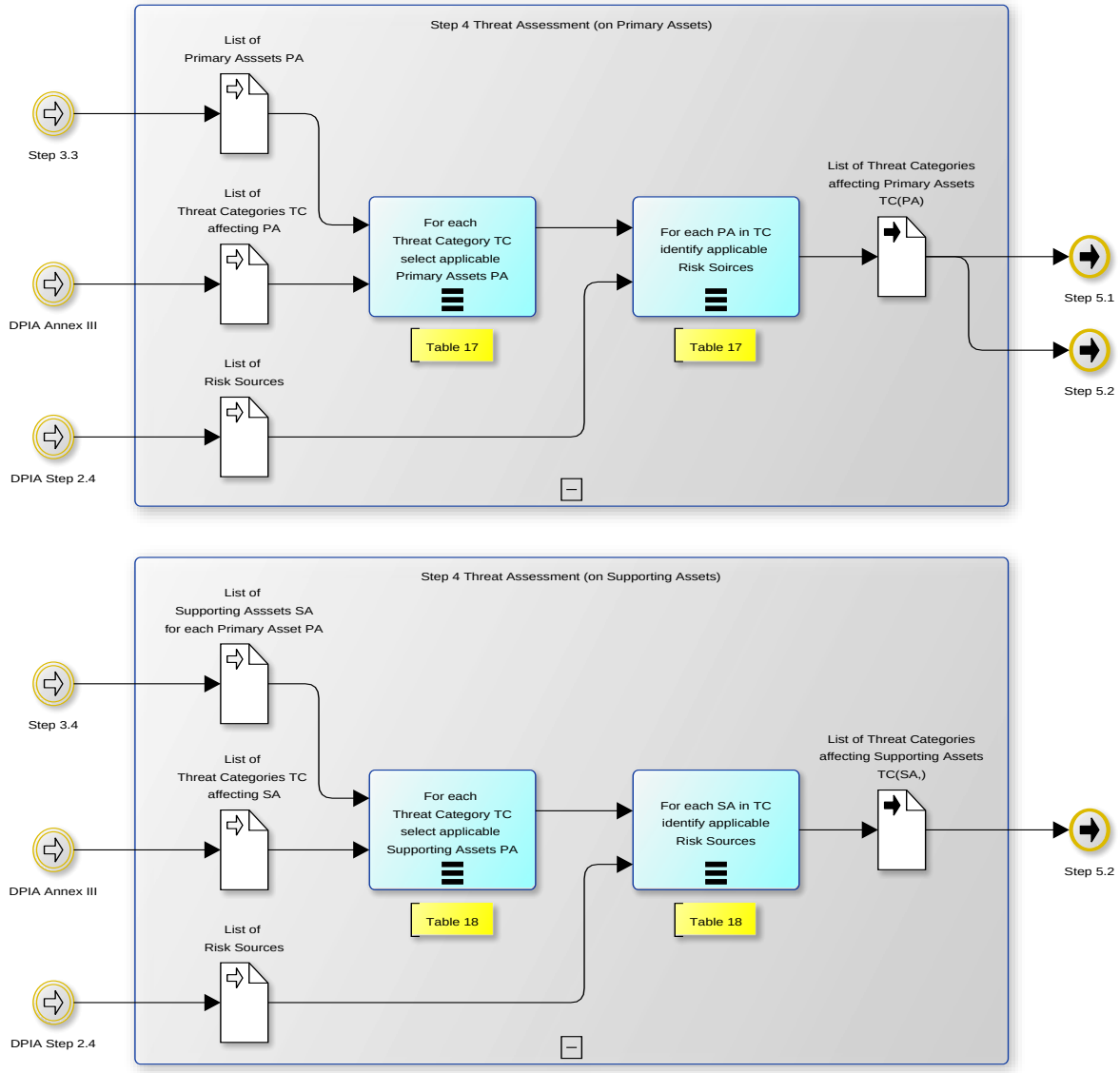


Figure 4. Threat Assessment Workflow

Tables in section 3.4 provide a listing of Threat Categories with possible assets involved and sources.

Annex III on Threat Taxonomy provides further guidance to the identification of the Threats.

Output > Step 5.1, Step 5.2
List of Threat Categories affecting Primary Assets TC(PA)
Output > Step 5.2
List of Threat Categories affecting qualified Supporting Assets TC(SA)

2.5. Step 5 – Risk Valuation

This step is aimed at determining the level of Risk associated to each Threat Categories affecting Primary Assets identified in step 4. The Risk level is weighted against two metrics:

- the **Severity** of impact that the Threat Category would have on the rights and freedoms of individuals, if the associated Threats become real; and
- **Likelihood** of the associated Threats to become real.

At the end of this step, a map of Threat Categories on the Severity vs Likelihood quadrant is obtained. Having this map will enable the subsequent step of deciding which actions to take for managing the Risk associated to each Threat Category.

In order to classify the Severity and Likelihood several widely available models can be used. The illustrative model for classification which is proposed and detailed below is mainly based on ISO 31000, EBIOS methodology and the synthesis produced by the CNIL[34], the French Data Protection authority. However, it is acceptable to use an alternate different methodology, either industry standard or internal ones, as long as the Risks that can impact the Data Subjects are properly identified and quantified.

2.5.1. Assessment of Severity

Step 4 > Input
List of Threat Categories affecting Primary Assets
Annex I > Input
List of GDPR Requirements

The Threat Categories are ranked by determining their **Severity** based on:

- the **Level of Identification** of Personal Data; and
- the **Prejudicial Effect** of these potential impacts.

The Severity is first evaluated for each Primary Asset associated to each Threat Category, and then the Severity at Threat Category level is determined. Given the list of Threat Categories affecting Primary Assets determined as the output of Step 4, the first task to perform is to assess, for each Primary Asset of each Threat Category, the **Level of Identification** of the Personal Data residing on the Primary Asset: how easy is it to identify an individual should the Threat gain access to the Personal Data residing on the Primary Asset?

Level of Identification of Primary Assets is evaluated based on the following scale:

1.	**Negligible:** Identifying an individual using its Personal Data appears to be virtually impossible (e.g. searching throughout a Member State population on one meter reading).
2.	**Limited:** Identifying an individual using their Personal Data appears to be difficult but is possible in certain cases (e.g. searching throughout a Member State population using an

[34] http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

	individual's 1-day history of meter readings).
3.	**Moderate:** Identifying an individual using their Personal Data appears to be common (e.g. searching throughout a Member State population using an individual's 1-week history of meter readings).
4.	**Significant:** Identifying an individual using their Personal Data appears to be relatively easy (e.g. searching throughout a Member State population using an individual's history of meter readings of multiple days).
5.	**Maximum:** Identifying an individual using their Personal Data appears to be extremely easy (e.g. searching throughout a Member State population using an individual's history of meter readings).

The value (1,2,3,4,5) of the Level of Identification that best matches the Primary Asset identified is selected (Table 19). Any existing or planned measures that reduce the identification should be documented and will be taken into account in Step 6. Subsequently, the **Prejudicial Effect is evaluated**.

Given the list of Threat Categories affecting Primary Assets determined as the output of Step 4, the second task to perform is to assess the **Prejudicial Effect** i.e. the potential impact on the rights and freedoms of the data subject if the threats associated to the category become real. This is done by evaluating, for each Primary Asset of each Threat Category, the potential impact of the associated Threats on rights and freedoms of natural persons, including those protected by the GDPR Requirements listed in Annex I.

Examples of impact on rights and freedoms of natural persons: include crime related Risks such as identity theft and fraud, or loss of the freedom to move, loss of independence, loss of equal treatment, intrusion on social relationships and financial interests, etc. due to e.g. profiling, unsolicited marketing, discrimination or individual decisions based on wrong information. The potential impact from Threats may extend beyond the directly affected individuals, causing **collateral damage to others**. This should also be considered in the Prejudicial Effect assessment.

Prejudicial Effect is evaluated based on the following scale:

1.	**Negligible:** Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2.	**Limited:** Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3.	**Moderate:** Data subjects may encounter consequences, which they will be able to overcome (extra costs due to denial of access to business services, delay, fury, minor physical ailments, etc.).
4.	**Significant:** Data subjects may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of state of health, etc.).
5.	**Maximum:** Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

The value of Prejudicial Effect is evaluated for each Primary Asset by performing the following tasks:

Considering the list of Threat Categories affecting Primary Assets
Considering the Primary Assets associated to each Threat Category
For each Primary Asset, identify relevant rights and freedoms of natural persons, including those protected by GDRP requirements from Annex I
For each right or freedom, associate the value of the level (1, 2, 3, 4, 5) that best matches the Prejudicial Effect i.e. the potential impact of that Threat Category on that GDPR requirement: if the Threats in the Category become real, how critical are the consequences for a particular right or freedom?
For each Primary Asset, determine the Prejudicial Effect as the maximum value of Prejudicial Effect evaluated for the applicable GDPR requirement

The last task of this process is to determine the Severity of each Threat Category. This is accomplished using the following procedure (Table 22):

For each Primary Asset of each Theat Category, Level of Identification and Prejudical effect are summed
The value resulting from the sum is normalized into a scale of 1 to 5 using Table 21: the result of this normalization is the Severity at Primary Asset level
Severity at Threat Category level is calculated as the maximum value of Severity of all associated Primary Assets.

When determining the final value of Severity, please be careful in assigning a value of 1, since Threats Category having a Severity < 2 will be not be subject to Likelihood analysis and will be assigned a conventional value of Likelihood = 1. As a consequence to this, if all Threat Categories to which a Primary Asset is associated have a normalized Severity of 1, then it is not needed to analyse Supporting Assets for that Primary Asset.

For each Threat Category having Severity >= 2, it is requested to perform Likelihood analysis (step 5.2), otherwise it is possible to proceed to Final Risk Level Assessment assigning to the Threat Category a conventional normalized Likelihood value = 1 (step 5.3). This task is described in *Figure 5*.

The workflow for this Step is pictured in the following diagram.

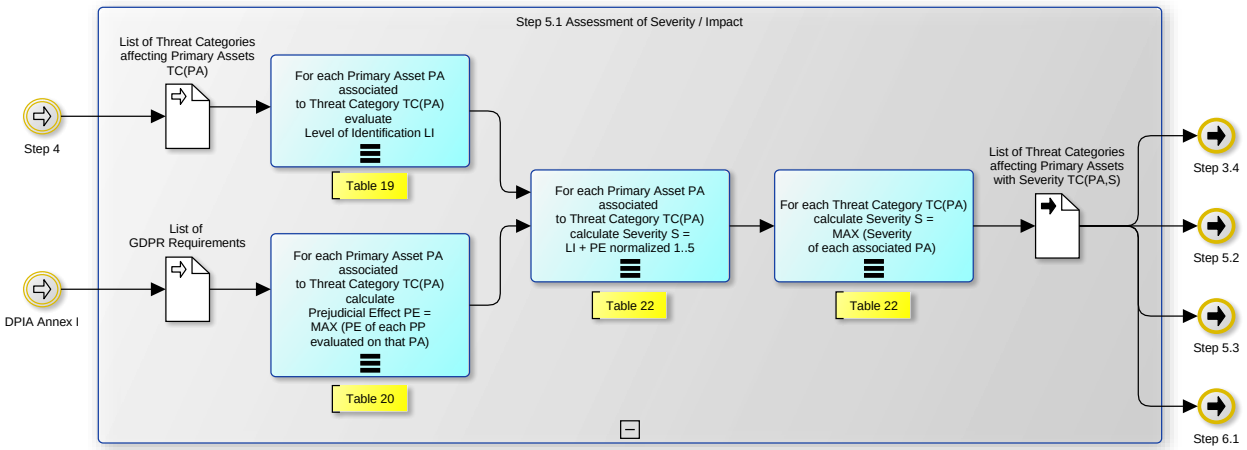


Figure 5 – Workflow for Assessment of Severity

Output > Step 3.4, Step 5.2, Step 5.3, Step 6.1
List of Threat Categories affecting Primary Assets with Severity TC(PA,S)

2.5.2. Assessment of Likelihood

Step 5.1 > Input
List of Threat Categories affecting Primary Assets with Severity TC
Step 4 > Input
List of Threat Categories affecting Primary Assets
Step 4 > Input
List of Threat Categories affecting Supporting Assets

Since Likelihood assessment is focused on Supporting Assets, the following tasks must be performed in order to obtain the necessary input information i.e. the List of Threat Categories affecting Supporting Assets:

Considering Threat Categories having a Severity value >= 2 resulting from Step 5.1 Severity Assessment;
For these Threat Categories, considering all associated Primary Assets;
For these Primary Assets, performing Step 3.4 *Characterization of Supporting Assets;*
For each Supporting Asset analysed in Step 3.4, performing Step 4 *Threat Assessment*, in order to determine which Threat Categories may affect it.

The output of this procedure is the List of Threat Categories affecting Supporting Assets The **Likelihood** of each Threat Category is assessed by the combination of:

- the **Level of Vulnerability** of the Supporting Assets associated to the Threat Category; and
- the **Capability of the Risk Sources** for the exploitation of this Vulnerability.

The Likelihood is first evaluated for each Supporting Asset associated to each Threat Category, then the Likelihood at Threat Category level is determined.

Given the list of Threat Categories affecting Supporting Assets determined as the output of Step 4, the first task to perform is to assess, for each Supporting Asset of each Threat Category, the **Vulnerability** of the Supporting Assets to the threats belonging to the Threat Category: how easy is it for the threats to exploit the vulnerabilities of the Supporting Asset? The **Vulnerability of Supporting Assets** is evaluated based on the following scale:

1.	**Negligible:** Carrying out a Threat by exploiting the Vulnerabilities of Supporting Assets does not appear possible (e.g. theft of paper documents stored in a room protected by a badge reader and access code).
2.	**Limited:** Carrying out a Threat by exploiting the Vulnerabilities of Supporting Assets appears to be difficult (e.g. theft of paper documents stored in a room protected by a badge reader).
3.	**Moderate:** Carrying out a Threat by exploiting the Vulnerabilities of Supporting Assets appears to be common (e.g. theft of paper documents stored in a room protected by a master key).
4.	**Significant:** Carrying out a Threat by exploiting the Vulnerabilities of Supporting Assets appears to be possible (e.g. theft of paper documents stored in offices that cannot be accessed without first checking in at reception).
5.	**Maximum:** Carrying out a Threat by exploiting the Vulnerabilities of Supporting Assets appears to be extremely easy (e.g. theft of paper documents stored in a lobby).

The value of the level (1,2,3,4,5) that best matches the Vulnerability of each Supporting Asset is then selected; for the subsequent tasks of this Step, it is useful to keep track of the Primary Assets to which each Supporting Asset is associated (Table 23). Control measures which are already implemented or planned for the system/application and which should in principle reduce these vulnerabilities and impact the value of this level will be taken into account in Step 6. Then the **Risk Sources Capability** is estimated.

Given the list of Threat Categories affecting Supporting Assets determined as the output of Step 4, the second task to perform is to assess, for each Supporting Asset of each Threat Category, the **Capability of Risk Sources:** how good are the Risk Sources applicable to each Supporting Asset at exploiting the vulnerabilities of the asset? The list of Threat Category affecting Supporting Assets (Table 18) also includes Risk Sources identified for each Supporting Asset.

The Risk Sources Capability is evaluated based on the following scale:

1.	**Negligible:** Risk Sources do not appear to have any special capabilities to carry out a Threat (e.g. software function creep by an individual acting without malicious intent and who has limited access privileges).
2.	**Limited:** The capabilities of Risks Sources to carry out a Threat are limited (e.g.: software function creep by a malicious individual with limited access privileges).
3.	**Moderate:** The capabilities of Risk Sources to carry out a Threat are common (e.g. software function creep by a malicious individual with limited administration privileges).
4.	**Significant:** The capabilities of Risk Sources to carry out a Threat are real and significant (e.g. software function creep by an individual acting without malicious intent and who has unlimited administration privileges).
5.	**Maximum:** The capabilities of Risk Sources to carry out a threat are defined and unlimited (e.g. software function creep by a malicious individual with unlimited administration privileges).

The value of the level (1,2,3,4,5) that best matches the Risk Sources capabilities is then selected for each Supporting Asset and for each Threat Category (Table 24). Any existing or planned measures that reduce the Capabilities of risk sources should be documented and will be taken into account in next Step 6.

The next step is to determine the Likelihood of Supporting Assets; this is done performing the following tasks:

All Supporting Assets associated to the Threat affecting Supporting Assets are listed in table 26;
For each Supporting Asset, the value obtained for the Vulnerabilities of the Supporting Assets and the one related to Capabilities of the risk sources are summed
The value obtained from the sum is is normalized into a scale of 1 to 5 using Table 25.
If a Supporting Asset is associated to multiple threats and has more than one entry in the table, then the value of Likelihood is the maximum between all the occurrences of that asset.

Once the Likelihood for all Supporting Assets being threatened has been calculated, the final step is to calculate the Likelihood for each Threat Category affecting Primary Assets. This is achieved applying the following procedure (Table 27):

Considering the List of Threat Categories affecting Primary Assets resulting from Step 4 and used as input for evaluating Severity.
For each Threat Category, considering the associated Primary Assets
For each Primary Asset, considering the associated Supporting Assets resulting from Supporting Assets Characterization (Step 3.4) – see Table 14.
If the Supporting Asset has an associated value of Likelihood (i.e. is listed in Table 26), listing it in Table 27
Calculating the Likelihood for each Threat Category (affecting Primary Assets) as the maximum Likelihood among all the associated Supporting Assets.

A detailed workflow for this Step explaining all tasks is pictured in the following diagram.

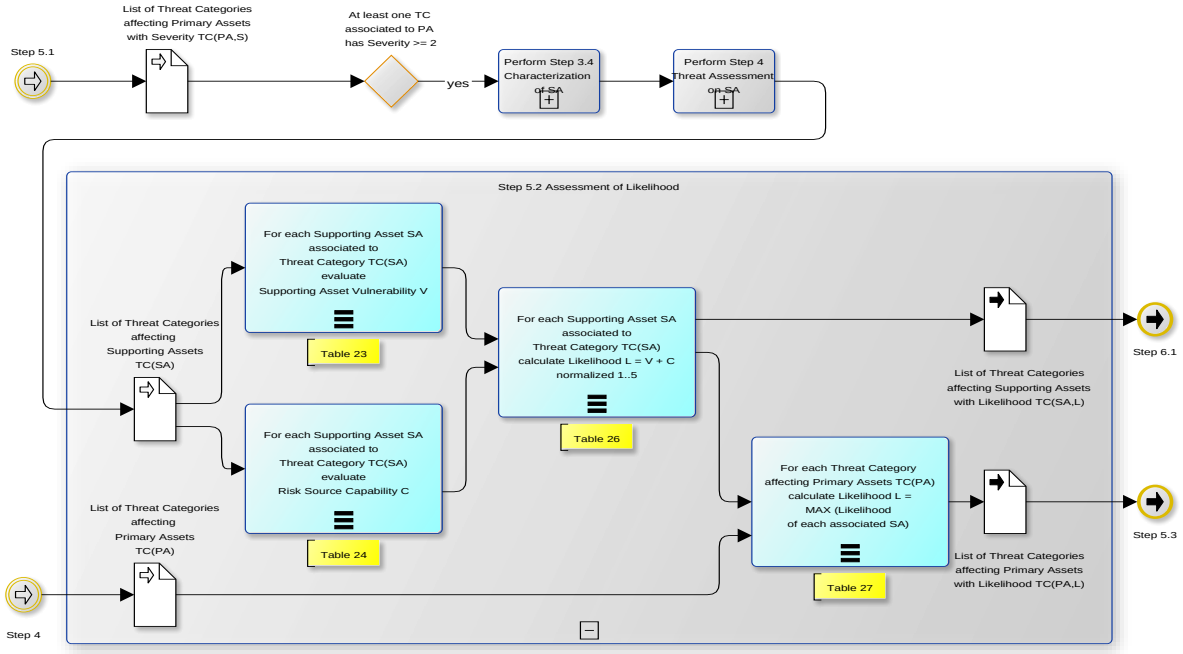


Figure 6 – Workflow for Assessment of Likelihood

Output > Step 5.3
List of Threat Categories affecting Primary Assets with Likelihood TC(PA,L)
Output > Step 6.1
List of Threat Categories affecting Supporting Assets with Likelihood TC(SA,L)

2.5.3. Assessment of Final Risk Level

Step 5.1 > Input
List of Threat Categories affecting Primary Assets with Severity TC(PA,S)
Step 5.2 > Input
List of Threat Categories affecting Primary Assets with Likelihood TC(PA,L)

At this stage of the analysis, each Threat Category affecting Primary Asset has been evaluated with two scores: Severity (Table 22) and Likelihood (Table 27). These two values are used as coordinates to place each Threat Category on the Risk Quadrant (Figure 9) where the Severity is the Y-axis and the Likelihood is the X-axis. These coordinates represent the Final Risk Level of the Threat Category.

Based on the zone of the Risk Quadrant where the Threat Category has been placed, a specific order of Priority is assigned to the Threat Category: this is the priority with which the Threat Category should be treated in the subsequent Step 6 about Risk Management. A lower order of Priority means a more serious Threat and a higher Risk.

The order of Priority is calculated from the value of the Final Risk Level, i.e. the (Likelihood, Severity) coordinates in the Risk Quadrant, according to the following scale:a:

1. Risks with a maximum/significant Severity and Likelihood: these risks must be absolutely avoided or reduced by implementing controls that reduce both their Severity and their Likelihood. Ideally, care should even be taken to ensure that they are treated by independent controls of prevention (actions taken prior to a damaging event), protection (actions taken during a damaging event) and recovery (actions taken after a damaging event)
2. Risks with a maximum/significant/moderate Severity but a negligible/limited/moderate Likelihood: these risks must be avoided or reduced by implementing controls that reduce both their Severity and their Likelihood. Emphasis must be placed on preventive controls. These risks can be taken, but only if it is shown that it is not possible to reduce their Severity and if their Likelihood is negligible
3. Risks with a negligible/limited Severity but a maximum/significant/moderate Likelihood and risks with a negligible/limited/moderate Severity but a maximum/significant Likelihood: these risks must be reduced by implementing controls that reduce their Likelihood. Emphasis must

be placed on recovery controls. These risks can be taken, but only if it is shown that it is not possible to reduce their Likelihood and if their Severity is negligible

4. Risks with a negligible/limited Severity and Likelihood: it should be possible to take these risks, especially since the treatment of other risks should also lead to their treatment.

The resulting value of Final Risk Level and Priority for each Threat Category is captured in Table 28. The diagram below provides guidance for this step.

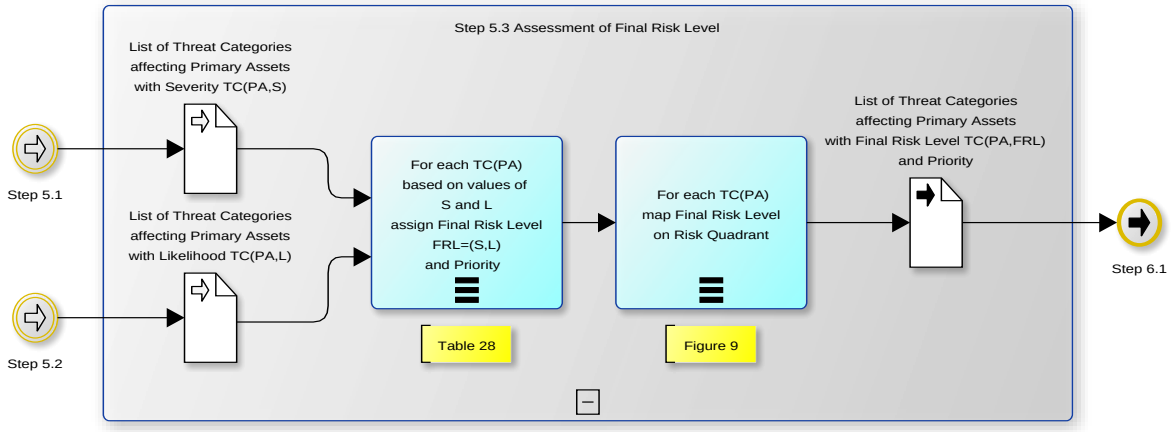


Figure 7 –Workflow for Assessment of Final Risk Level

Section 3.5 provides template tables for each step of the Risk Assessment. At this stage, the controls and mitigation measures implemented and planned are still not taken into account in the evaluation of the Final Risk Level.

Output > Step 6.1
List of Threat Categories affecting Primary Assets with Final Risk Level and Priority TC(PA,FRL)

2.6. Step 6 - Risk Treatment and Final Resolution

2.6.1. Assessment of Residual Risk Level

Step 5.1 > Input
List of Threat Categories affecting Primary Assets with Severity
Step 5.2 > Input
List of Threat Categories affecting Supporting Assets with Likelihood
Step 5.3 > Input
List of Threat Categories affecting Primary Assets with Final Risk Level and Priority
DPIA Annex II > Input
List of possible Controls

2.6.1.1. Identification of implemented and planned Controls

At this stage, the aim is to consider the Risks identified and assessed in the previous Step and to present which controls have been, or are planned to be, implemented in order to reduce the risk at appropriate levels. Each identified Risk needs to be appropriately mitigated operating in line with the requirements of the General Data Protection and on one or more controls (see

Annex II – List of Possible Controls), considering the Likelihood and Severity indicators.

In order to assist the proliferation of the best mitigation measures, the EG2 is establishing a list of 'Best available techniques' in Smart Metering system environments which can provide further guidance to the Data Controller regarding which Control will be the most efficient.

Best Available Techniques as defined in the point 3.f of the Recommendation[35], refers to "*the most effective and advanced stage in the development of activities and their methods of operation, which indicate the practical suitability of particular techniques for providing in principle the basis for complying with the EU Data Protection framework. They are designed to prevent or mitigate risks on privacy, Personal Data and security.*"

The Controls adopted or already planned by the Data Controller should cover the following dimension, all being related to Supporting Assets:

- The infrastructure (communication network, Equipment Protection, hardening, etc.);
- The agents/personnel involved in the process (individual access and control mechanism, etc.);
- The organisation and procedure (Smart Grid application governing practices, accountability measures, etc.);
- The technologies (system protection measures including Security Controls and IT based security methodology, etc.).

The DPIA report should explain in detail how the selected (implemented or planned) Controls relate to specific Risks, and should demonstrate that they result in acceptable Risk levels. When the Risk is shared with a third party, the Data Controller should also detail which Control this third party has implemented or planned to implement in order to address this Risk in an acceptable way.

It is also recommended to design and implement an internal process (see: Step 8) with the aim of regularly verifying if identified Controls are in place (e.g. performing audits on a regular basis, which is the ultimate Control listed in the List of Controls in Annex II).

2.6.1.2. Risk Treatment

Having identified and assessed the risks, the Data Controller needs to specify the way these Risks will be managed. This can be done with the inclusion of a table in part 3.6 where Risk Treatment techniques to manage Risks on Primary Assets can be described. In this table the Data Controller should also demonstrate compliance with the GDPR Requirements. Such compliance might be demonstrated through the internal compliance mechanisms of the Smart Grid operator.

The possible options which can be adopted to manage those risks are proposed below:

- **Risk Modification**: The risk is managed by identifying and introducing additional (to those already implemented or planned and described in section 2.6.1) appropriate controls, thereby reducing the risk to acceptable levels;

[35] Commission recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (COM 2012/148/EU

- **Risk Retention**: The Data Controller accepts the Risk as it is, if it meets the acceptance criteria, without any further action;
- **Risk Avoidance**: The Data Controller decides not put the application in production;
- **Risk Sharing**: The Risk is shared with a third party, which can manage the identified Risk more effectively and thereby reduce the risk to acceptable levels.

It is noted that these options are not mutually exclusive. The Data Controller may decide to go with more than one option. Further details should be added to the report regarding the approach undertaken. The following information should be at least included:

- Appropriate justification for the selection of specific option(s) for treating the Risk and proposed approach to ensure that the risk will be monitored to make sure acceptance is appropriate in light of the evolving external landscape (e.g. Threats, Vulnerabilities, legal requirements etc.). Ideally the Data Controller should perform a cost benefit analysis when selecting among these options, considering the expected benefits and costs of implementing each option;
- Consultation of the Data Protection Officer (DPO) when available;
- Date: The decision was approved (this should include history demonstrating each time the action was taken);
- Date of next review if already planned;
- External Review: Any details of this document being reviewed (with comments) from third party review.

2.6.1.3. Residual Risks and Risk acceptance

According to ISO 27005[36], the Residual Risk is "the risk remaining after the risk treatment". In this context, the Data Controller needs to identify appropriately the Residual Risks that remain after implementing controls. When those are identified (in the previous step), the Data Controller would then need to decide whether additional Controls would need to be implemented to address those Residuals Risks considered as still unacceptable.

Finally, based on this analysis and the acceptance levels set by the management, the decision to accept those Risks may need to be made. The decision:

should be appropriately and carefully justified, especially in the case when risks that don't fall within the acceptable levels are at any rate accepted (e.g. because it is not considered cost-efficient to address them, in view of the advantages associated with the risk etc.);
may adopted only if it is demonstrated that the benefits of processing greatly outweigh the risks for the individual;
must be compliant with the provisions of the General Data Protection Regulation i.e. independently of the outcome of this risk assessment, it has to be underlined that General Data Protection

[36] An information security standard published by the International Organisation for Standardization (ISO) and the International Electro technical Commission (IEC); information security should be understood as Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

requirements (as listed in Annex I) have to be complied with, .e.g. the processing operations need to be always supported by a lawful ground.

E.g. An unencrypted data exchange which had a high risk of privacy breach is addressed by implementing a cipher suite in the platform to ensure confidentiality. However, due to technology and cost limitations the encryption algorithm is not that strong and proven to be vulnerable to brute force attacks. The initial risk has been addressed; however, there are still residual risks. For instance, the implemented Control itself may be broken. Over time it might happen that the encryption algorithm will become less secure and will have therefore an impact on the level of the residual risk. However the Likelihood that this is happening increases in time.

The expected result of this task is a list of planned and implemented Controls for mitigating the identified risks on Supporting Assets, of Risk Treatment techniques for mitigating Risks on Primary Assets, and a new risk map with the residual risks located (part 3.6) In principle this new risk map should have Residual Risks at a lower level compared to the first risk map with no controls

A proposed workflow for approaching this Step is provided by the diagram below, with matching tables in section 3.6. However, any Risk Mitigation methodology endorsed by the Smart Grid Operator can be used in order to identify and describe Controls and Risk Treatment techniques, and determine the Residual Risk Level for each identified Threat Category affecting Primary Assets.

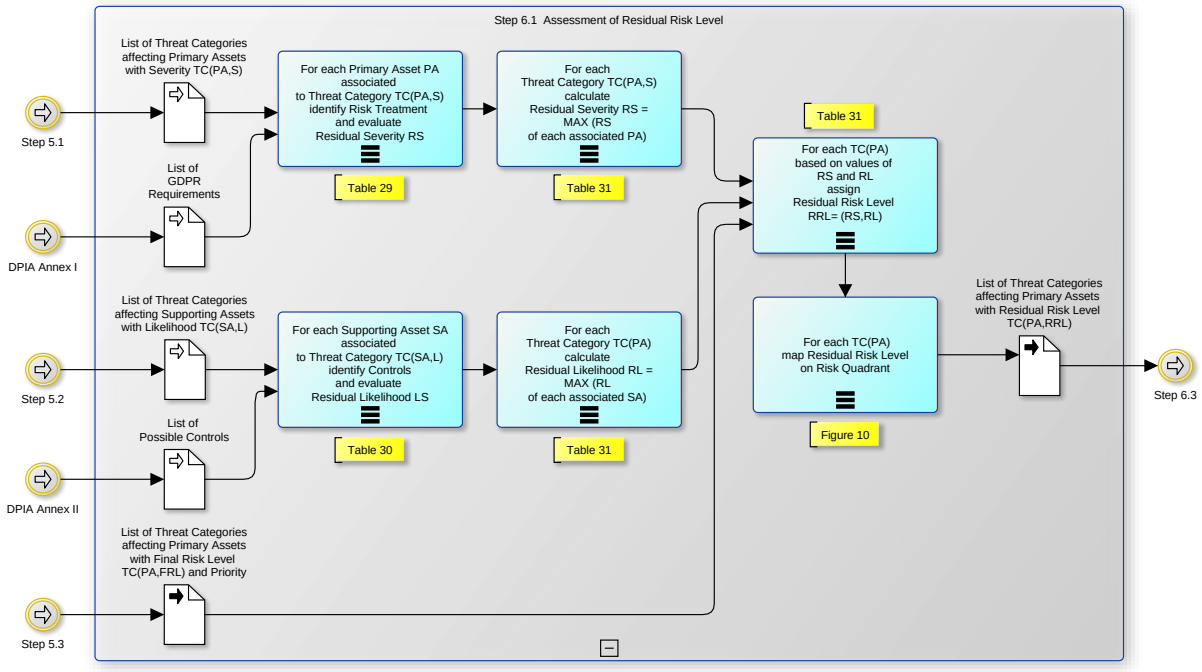


Figure 8 –Workflow for Assessment of Residual Risk Level

Output > Step 6.3
List of Threat Categories affecting Primary Assets with Residual Risk Level TC(PA,RRL)

2.6.2. GDPR Requirements' Coverage Check

In order to:

(i) provide assurance that the Threat and Risk Assessment carried out on the Smart Grid project targeted by the DPIA properly address the goals of the GDPR;

(ii) demonstrate compliance in accordance with Art. 35 (7) of the GPDR;

a final, end-to-end crosscheck against GDPR Requirements shall be performed for each Use Case in scope for the DPIA after determining the Residual Risk.

Step 3.1 > Input
List of Use Cases involving Personal Data

The final check is done by filling the table in section 3.6.2 listing all Use Cases in scope for the DPIA and, for each of them, the relevant GDPR Requirements. For each line a yes/no answer should be given if a requirement is fulfilled or not at end-to-end level for that Use Case. Rationales about how the requirements for each Use Case are fulfilled shall also be provided in the final check. With regard to the basic principles of Data Processing, set out in art. 5 of the GDPR, the rationale behind assuring compliance should be elaborated at a higher level of detail as set out in Annex I. Please note that it may be the case that some GDPR requirements are not applicable, for instance because no special categories of data are processed or there is no automated-decision making.

When performing the final end-to-end assessment, the DPIA team must remember that a requirement is fulfilled at Use Case level only if a requirement is fulfilled for every Primary Asset associated to the Use Case, since requirements apply to Personal Data and Primary Assets are the realization of Personal Data and related Processing operations for each Use Case. For this task, the mapping between Primary Assets and Use Cases in table 11 and the assessment of Prejudicial Effect (related to impact of Threat Categories on right and freedoms of natural persons) in table 20 will be useful.

A well-performed personal Data Protection risk management process should conclude with no relevant GDPR Requirements left uncovered. If the resulting crosscheck includes any “no” answer to a major requirement, the DPIA team should consider revising the risk management until all the GDPR Requirements are covered.

Output > Step 6.3
GDPR Requirements' Coverage Check

2.6.3. Final Resolution

The DPIA process should conclude with a resolution based on the results of the risk management process that has been performed, as well as on the Residual Risks and the decision to accept risks or not (based on a cost-benefits analysis as well).

Matching of all of the relevant GDPR Requirements to each Primary Asset should also be a precondition for this decision.

Step 6.1 > Input
List of Threat Categories affecting Primary Assets with Residual Risk Level
Step 6.2 > Input
GDPR Requirements Coverage Check

The DPIA on a Smart Grid application or system is complete once all relevant Risks are properly identified and mitigated and residual high risks for the individuals (resulting from step 6.3) are addressed via prior consultation with the DPA, in line to the GDPR art. 36. All the documentation must be accompanied by internal reviews and approvals demonstrating that the Data Controller evaluated risks and countermeasures involving the processes responsible and experts.

The following resolutions can be envisaged at the end of the DPIA process, in case of:

- A Smart Grid system or application already in production:
    - if the Controller considers the Risks as mitigated: the DPIA reports should be registered and stored by the Data Protection Officer (if any) of the organisation and kept at the disposal of Data Protection Authority;
    - if the Data Controller considers the mitigation insufficient: in case high Risks are highlighted, the controller shall consult the supervisory authority accordingly to GDPR art. 36. Further consideration will require a specific corrective action plan to be developed including proposal for more efficient or new controls and a new DPIA to be completed in order to determine if the mitigation is finally effective.
- A Smart Grid system or application still under design:
    - if the controller considers the Risks as mitigated : Risks have been assessed and controls addressing those Risks properly defined and tuned. The system implementation proceeds. The DPIA report should include future dates for checking the system when it will be in production.
    - if the controller considers the mitigation insufficient: in addition to envisage further controls for obtaining a new and satisfactory level of Residual Risks, the report should also recommend when possible, new design actions for the application following the principle of Data Protection by Design[37]. When the system activation is mandatory despite high Risks emerged from the DPIA, the controller shall consult the supervisory authority accordingly to GDPR art. 36.

It is important to note that the final resolution should be a Data Controller decision and it should be based on the results of the assessment performed including and reflecting the societal stakes related to the development of Smart Grid.

[37] Implementing technical and organisational measures which are designed to implement Data Protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

Output
Final Resolution made by the Data Controller, related to considering the Residual Risks acceptable or needing further assessment.

2.7. Step 7 - Documentation and drafting of the DPIA Report

The execution of the DPIA should be appropriately documented and its results presented in the final DPIA report. It shall be structured following the step-by-step approach described in the Template, presenting the results of each phase to the reader, and annexing any supporting documents or material used in the assessment.

Since DPIAs are internal processes which may handle proprietary classified information of the Smart Grid operator related to products and processes, they might entail special confidentiality requirements. As such, the analysis performed and its documentation may need to be appropriately secured, in accordance with the organisation's information classification scheme.

The signed DPIA Report that contains an approved resolution should be given to the assigned organisation's Data Protection Officer in accordance with the Smart Grid operator's internal procedures. The Data Protection Officer will keep an administration of the signed DPIA reports in case of (external) audits and/or inspection from the DPA.

The objective of the documentation is two-fold: (a) to facilitate the implementation of the process and (b) to produce a final report that could be submitted to the DPA if requested.

Output
The DPIA report that can be distributed to stakeholders when appropriate.

2.8. Step 8 - Reviewing and Maintenance

The purpose of this Step is to ensure that the Risk Treatment plan that arose from the conducted DPIA is carried out in the existing Smart Grid system(s) or implemented project.

The GDPR provides that the Data Controller shall carry out a review to assess if processing of Personal Data is performed in accordance with the DPIA at least when there is change of the Risk represented by processing operations. The review can be integrated with the organisation's standard, periodic or occasional internal processes.

The following tasks are suggested:

- A review of the implementation of the mitigation and avoidance Controls that were identified in the DPIA;
- Preparation of a review report;
- Presentation of the review report to the senior management and DPO where available;
- Making the review report publicly available;

ADPIA should not be a static *ad hoc* document. Consequently, there is a need for revising the DPIA after a certain amount of time or after a new stage within the Smart Grid project has been completed.

Output
DPIA Review Report **Recommendation on performing (or not) a new DPIA**

3. Questionnaires

3.1. Step 1 - Pre-assessment and criteria determining the need to conduct a DPIA

3.1.1. Criterion 1 – Cases foreseen by the GDPR, DPAs or the European Data Protection Board

- Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?
- Are you processing Personal Data on a large scale?
- Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?
- Are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?
- Is the designed Smart Grid application or system listed by my national Data Protection Authority or by the European Data Protection guidelines as one that requires DPIA?
- Is the designed Smart Grid application or listed by my national Data Protection Authority or by the European Data Protection guidelines as one that does not require DPIA?

3.1.2. Criterion 2 – Relevant occurrence

- Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?

3.1.3. Criterion 3 – Personal Data involved and DPIA-related Processing activities

- Does the design/change require you to collect and process any Personal Data, in particular detailed household consumption data, consumer registration data, etc.?
- Is the purpose or scope of the process capable to have an impact on the rights and freedoms of natural persons, e.g. household insights?

3.1.4. Criterion 4 – Status of a Data Controller or a Data Processor

- Are you the Data Controller or a Data Processor?
- Have Data Protection (contractual) requirements already been defined between you and the Processor/Controller?

3.1.5. Criterion 5 - New technologies and other criteria

- Does the Data Controller plan to implement new technologies for the considered process?
- Does the design/change contain any other criterion that may affect rights and freedoms of natural persons?

3.2. Step 2 - Initiation

3.2.1. Choice of the DPIA management option

- Please indicate whether DPIA will be performed by: (i) a dedicated DPIA team, (ii) a third party, (iii) the persons in charge of the Process/ Project, or (iv) other team.

3.2.2. Identification of DPIA team members

Table 2. Identification of DPIA team members

Team member name	Company	Organizational Role	Responsibility in DPIA Analysis

3.2.3. Inventory of necessary sources

Table 3. Inventory of necessary sources

Sources	Purpose	Steps of DPIA

3.3. Step 3 – Analysis of Use Case

3.3.1. Scope Definition

Table 4. Description of the target initiative of DPIA

Brief Description of the target initiative of DPIA

Table 5. List of Use Cases supported by the target initiative

Use Case ID	Use Case Name	Involves Personal Data (Y/N)

3.3.2. Characterisation of Use Case

For each Use Case involving Personal Data according to *Table above*, an instance of section 3.3.2 should be compiled.

3.3.2.1. Description of Use Case

Table 6. Description of Use Case

Use Case ID	
Use Case Name	
Domain and Zones	
Scope	
Short Description	

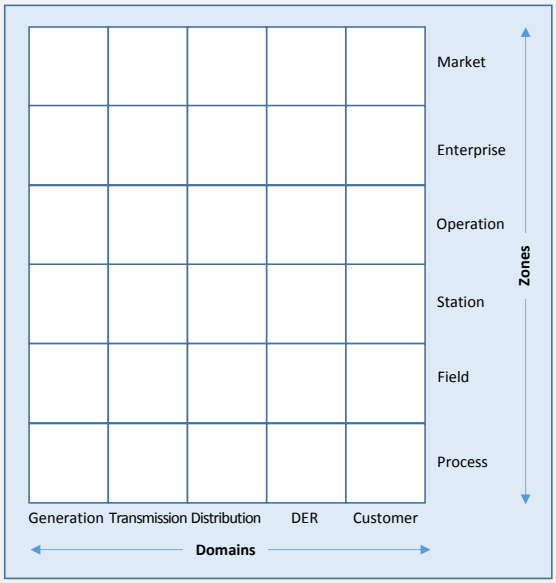
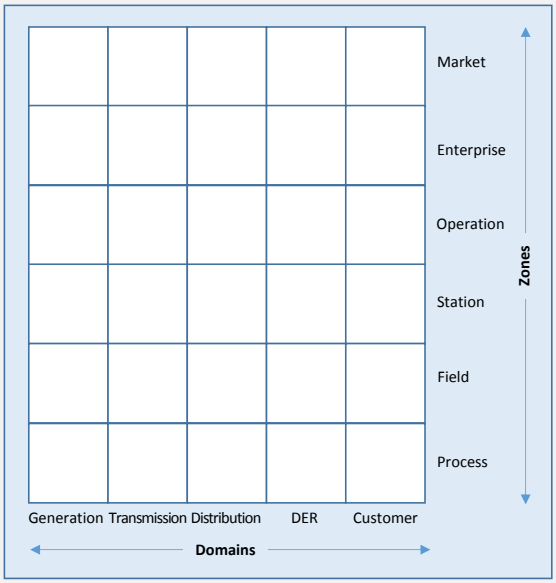
3.3.2.2. Description of Actors

Table 7. Description of Actors

Acronym	Actor name	Actor type	Actor description

3.3.2.3. Representation of Use Case on SGAM Layers (Diagrams)

Table 8. Representation of Use Case on SGAM Interoperability Layers

Representation on Component Layer	Representation on Communication Layer
	

3.3.2.4. Description of Scenarios (step-by-step analysis of Use Case)

Table 9. List of Use Case Scenarios involving Personal Data

Scenario ID	Scenario name	Scenario description	Primary Actor

For each Scenario listed in *Table above*, an instance of the following table should be compiled, containing one row for each Step of the Scenario.

Please note that Personal Data Processing Operation also include Personal Data exchange between different actors.

Table 10. Step-by-step description of Scenario related to Personal Data

Scenario ID and Name					
Step No.	**Description**	**Information producer (Actor)**	**Information receiver (Actor)**	**Personal Data involved**	**Personal Data Processing Operation performed**

3.3.3. Characterisation of Primary Assets

The following tables can be used to collect information for Primary Assets identified during the analysis of all Use Cases in scope involving Personal Data.

The three tables below can be seen as one table, as for each Primary Asset one row for each table should be filled, keeping the same Primary Asset ID value. Instead of the tables below, a spreadsheet file that would allow to unify the three tables into one (by pasting columns from the three tables side-by-side and keeping just one Primary Asset ID column) can also be used and referenced.

As explained in the Guidance section, a Primary Asset is Personal Data allocated on a specific Actor, so each different combination of Personal Data and Actor identified during the analysis of Scenarios will result in one row of the tables below.

Table 11. Description of Primary Assets/Actor

Reference		Actor			
Primary Asset ID	**Involved in: List of (Use Case ID – Scenario ID – Step No.)**	**Actor**	**SGAM Smart Grid Plane Coordinates (Domain/Zone)**	**Cardinality of Actor**	**Cardinality of Personal Data per Actor**

Table 12. Description of Primary Assets/Personal Data

	Personal Data				
Primary Asset ID	**Category of Personal Data**	**Data subject**	**Personal Data**	**Access Frequency within Actor**	**Retention time within Actor**

Please note that in the table below, Personal Data Processing operation also include Personal Data exchange between different Actors.

Table 13. Description of Primary Assets/Processing Operation

	Processing Operation						
Primary Asset ID	**Processing operation**	**Purposes of the processing**	**Necessity in relation to purposes**	**Proportionality in relation to purposes**	**Legal obligations for processing**	**Data Controller**	**Data Processor**

3.3.4. Characterisation of Supporting Assets

Fill a row for each Primary Asset identified at step 3.3.3. Fill only the columns applicable for that Primary Asset.

Table 14. Description of Supporting Assets

Supporting Assets								
	IT/OT Resources			Human Resources			Paper Resources	
Primary Asset ID	**HW**	**SW**	**Communication Network**	**Human Roles**	**Human Tasks**	**AAA mechanisms**	**Paper Media**	**Paper Transmission channels**

3.4. Step 4 – Threat Identification

In order to facilitate the identification of Threats, a list of Threat categories is provided below. Threats categories are grouped in two sets depending on the type of asset they may affect.

Threats evaluation on Primary Assets is mandatory. Data Protection Threat categories - Outcome of the Threat identification

Each Threat Category should be associated with one or more Primary Assets. Within the table below the selection of Threats identified on the basis of Threat Categories set out in Annex, should be listed:

Table 15. Threat Categories affecting Primary Assets with Risk Sources

Threat Category affecting Primary Assets	Primary Assets	Risk Source	Brief explanation why relevant
Violation of data subject's rights	*Primary asset 1* *i.e. measure-X*	*i.e. Outsider*	
	Primary asset 2		
	…		

The outcome below is required only when there have been identified Primary Assets with Severity >= 2 (high impact) as determined in step 5.1. In this case, it is requested to evaluate threat categories affecting only Supporting Assets related to high impact Primary Assets.

In the table below, each Threat Category should be associated with one or more Supporting Assets.

Table 16. Threat Categories affecting Supporting Assets with applicable and Risk Sources

Threat Category affecting Supporting Assets	Supporting Assets	Related Primary Asset	Risk Source
i.e. Physical damage	*Supporting asset 1* *i.e. concentrator-Y*	*i.e. measure-X*	*i.e. Outsider*
	Supporting asset 2		
	…		

3.5. Step 5 – Risk Valuation

3.5.1. Assessment of Severity

Table 17. Level of Identification per Threat Category affecting each Primary Asset

Threat Category affecting Primary Assets TC(PA)	Primary Asset	Level of Identification LI at PA Level
i.e. Information of the data subject	*A Primary Asset*	*i.e. 3*

Table 18. Prejudicial Effect per Threat Category affecting each Primary Asset

Threat Category affecting Primary Assets TC(PA)	Primary Asset PA	Rights and Freedoms of natural persons, including those protected by the GDPR	Prejudicial Effect PE at PT level	Prejudicial Effect PE at PA level
	i.e. Information of the data subject	*A GDPR requirement*	*i.e. 4*	*i.e. 4*
		Other right or freedom	*i.e. 2*	

Table 19. Severity Normalisation Scale

Level of Identification + Prejudicial Effects LI + PE	Severity
< 4	1. Negligible
4 or 5	2. Limited
= 6	3. Moderate
6 or 7	4. Significant
> 7	5. Maximum

Table 20. Severity of Threat Category affecting Primary Assets

Threat Category affecting Primary Assets TC(PA)	Primary Asset PA	LI + PE	Severity at PA level	Severity at TC level
i.e. Information of the data subject	*i.e. measure-X*	*3 + 4*	*3*	*4*
		2 + 3	*4*	

3.5.2. Assessment of Likelihood

Table 21. Vulnerability to a Threat Category of each Supporting Asset

Threat Category affecting Supporting Assets TC(SA)	Supporting Asset SA	Related Primary Asset PA	Supporting Asset Vulnerability V
i.e. Physical attack	*i.e. concentrator-Y*	*i.e. measure-X*	*2*

Table 22. Capability of a Risk Source to exploit the Vulnerability of each Supporting Asset

Threat Category affecting Supporting Assets TC(SA)	Supporting Asset SA	Risk Sources	Risk Source Capability C
i.e. Physical attack	*i.e. concentrator-Y*		*4*

Table 23. Likelihood Normalisation Scale

Supporting asset vulnerabilities + risk source capabilities	Likelihood
< 4	1. Negligible
4 or 5	2. Limited
= 6	3. Moderate
6 or 7	4. Significant
> 7	5. Maximum

Table 24. Likelihood of Supporting Assets

Supporting Asset SA	Related Primary Asset PA	V	C	V+C at SA level	Likelihood L at SA level
i.e. concentrator-Y	*i.e. measure-X*	*2*	*4*	*6*	*3*

Note: if Likelihood has not been assessed, as for Threat Categories having Severity <2 , then a conventional value of L = 1 must be used.

Table 25. Likelihood of Threat Categories affecting Primary Assets

Threat Category affecting Primary Assets TC(PA)	Primary Asset PA	Supporting Asset SA	Likelihood at SA level	Likelihood L at TC Level

3.5.3. Assessment of Final Risk Level

Table 26. Final Risk Level and Priority of Threat Categories affecting Primary Assets

Threat Category affecting Primary Assets TC(PA)	Severity S	Likelihood L	Final Risk Level (L, S)	Risk Priority
i.e. Information of the data subject	*5-Maximum*	*4-Significant*	*(4,5)*	*1*
	--			

Graphical presentation of the final Risk Levels determined on the Use Case (as-is):

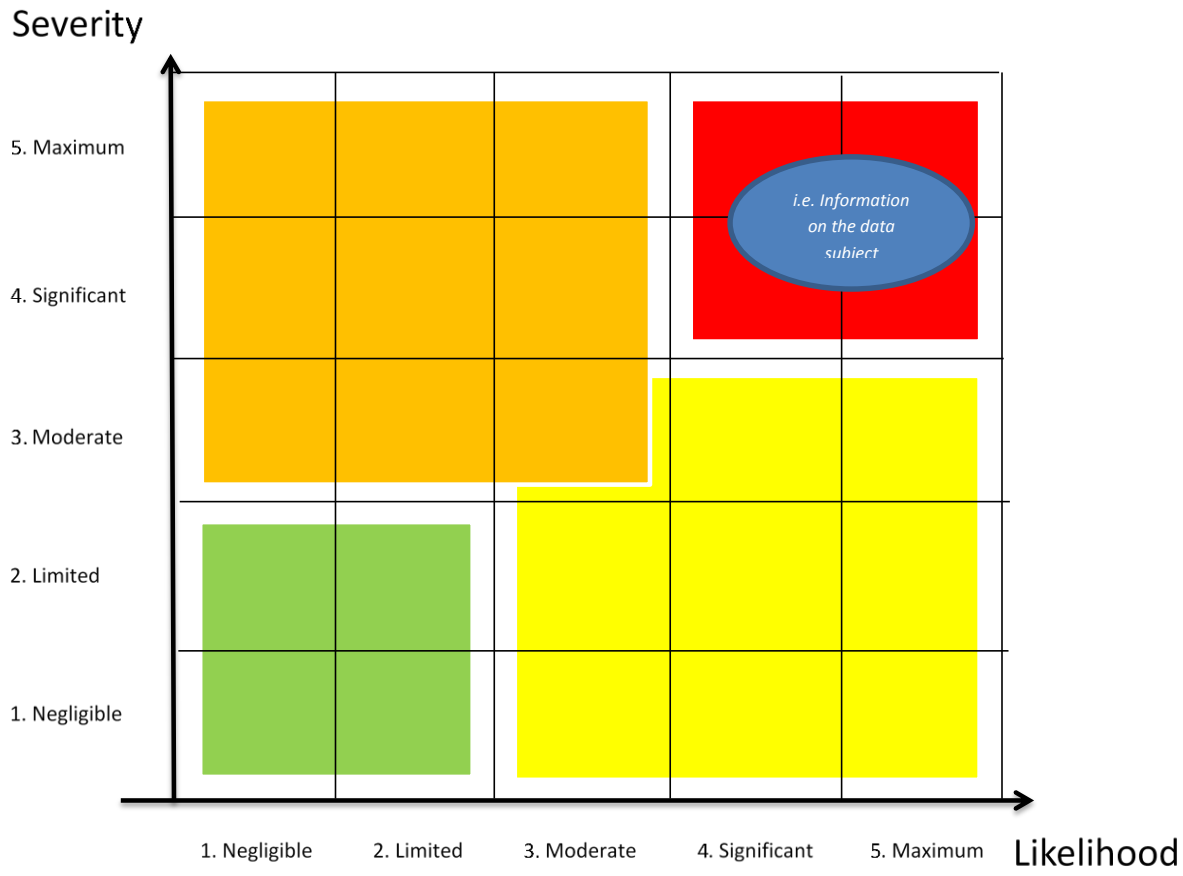


Figure 9. Risk Quadrant – Representation of Final Risk Level of Threat Categories affecting Primary Assets

3.6. Step 6 – Risk Treatment and Final Resolution

3.6.1. Assessment of Residual Risk Level

Table 27. Risk Treatment on Threat Categories affecting Primary Assets for mitigation of Severity

Threat Category affecting Primary Assets TC(PA)	Affected Primary Asset	Severity S	Risk Treatment (including assuring compliance with GDPR Requirements)	Residual Severity RS
i.e. Information on the data subject	*i.e. measure-X*	*3*	*i.e. processed lawfully, collected for specified, explicit and legitimate purposes, etc.*	*2*

Table 28. Identification of Controls on Threat Categories affecting Supporting Assets for mitigation of Likelihood

Threat Category affecting Supporting Assets TC(SA)	Affected Supporting Asset	Likelihood L	Controls planned or implemented	Residual Likelihood RL
i.e. Physical attack	*i.e. concentrator-Y*	*4*	*i.e. use Multifactor Auth*	*2*

Table 29. Residual Risk Level and of Threat Categories affecting Primary Assets

Threat Category affecting Primary Assets TC(PA)	Affected Primary Asset	Residual Severity RS at PA level	Residual Severity at TC level	Affected Supporting Asset	Residual Likelihood at SA Level	Residual Likelihood at TC Level	Residual Risk Level RRL = (RS,RL)
i.e. Information on the data subject	*i.e. measurement-X*	*2*	*2*	*A*	*2*	*2*	*(2,2)*
				B	*1*		
	i.e processing operation-Y	*1*		*C*	*1*		
				D	*1*		

Table 30. Summary of Final Risk Level, Priority and Residual Risk Level of Threat Categories affecting Primary Assets

Threat Category affecting Primary Assets	Final Risk Level	Priority	Residual Risk Level (RS,RL)

TC(PA)			
i.e. Information on the data subject	*4,4*	*1*	*(2,2)*

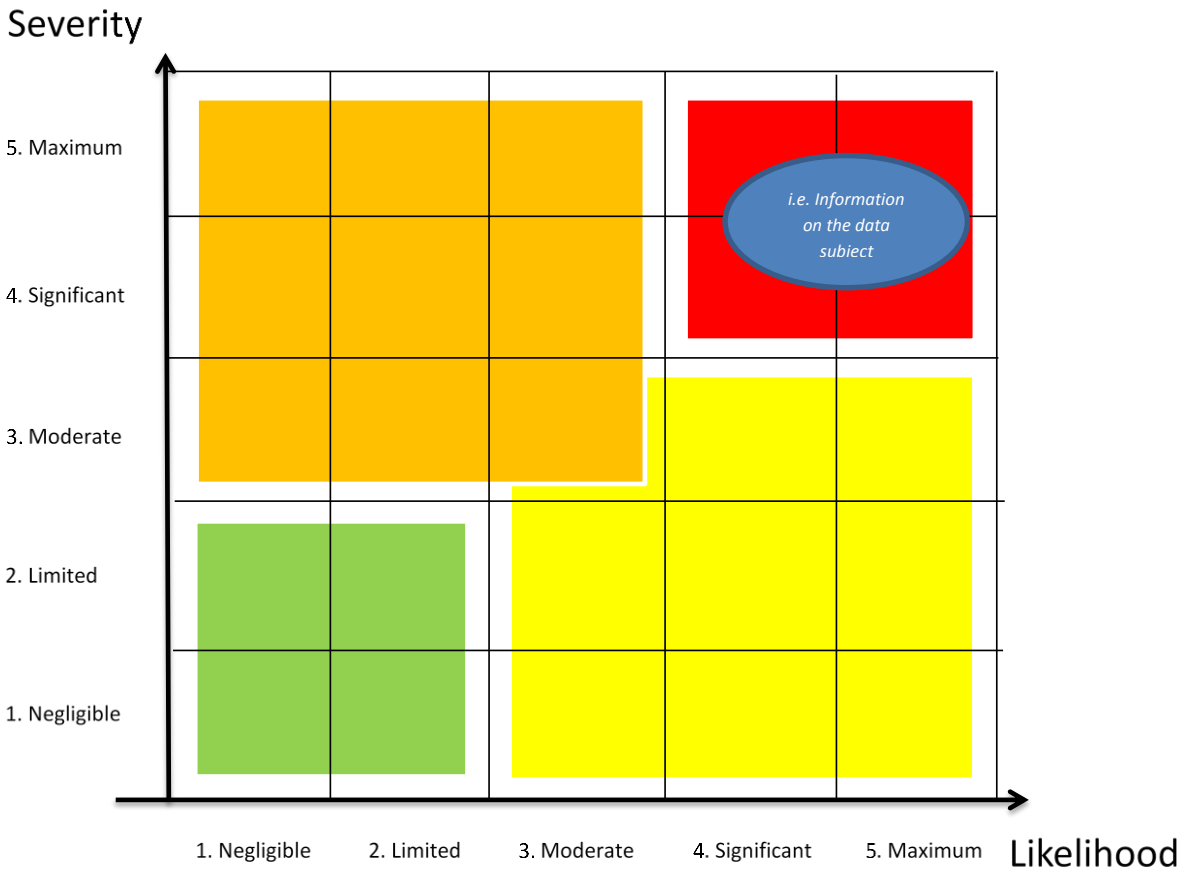


Figure 10. Risk Quadrant – Representation of Residual Risk Level of Threat Categories affecting Primary Assets

3.6.2. GDPR Requirements' Coverage Check

Table 31. Final check of GDPR requirements end-to-end coverage on each Use Case

Use Case UC	GDPR Requirements	Yes/No	Rationale
Use Case 1	Basic principles (art. 5)		
	Purpose Limitation		
	Data minimisation		
	Storage Limitation		
	Integrity and confidentiality		
	Other GDPR requirements		
	The processing is based on lawfulness conditions provided by GDPR [art. 6]		
Use Case 2			

ANNEXES

Annex I – GDPR Requirements

This Annex provides a basic checklist to help verify that the rules set forth in the GDPR have been complied with and to document how such compliance is achieved. It may be the case that some fields are not applicable, for instance because no special categories of data are processed or there is no automated-decision making.

Provisions	Yes/No	Rationale
The Principles relating to processing of Personal Data have been fulfilled [art.5]:		
Purpose Limitation		
Data minimization		
Storage Limitation		
Integrity and confidentiality		
Data is accurate and kept up-to-date		
The processing is based on Lawfulness conditions provided by GDPR [art. 6]		
Where the processing is based on consent, it is possible to demonstrate that the data subject has consented to processing of his or her Personal Data [art. 7]		
Processing of special categories of Personal Data is performed adopting all the measures provided by GDPR [art. 9]		
The controller provided information to the data subject [art.13,14]		
The right of access by the data subject is guaranteed [art. 15]		
The right to rectification is guaranteed [art. 16]		
The right to erasure is guaranteed [art. 17]		
The right to restriction of processing is guaranteed [art .18]		
Has ever been sent to the recipients of the Personal Data a notification when the data subject requested a rectification, erasure or restriction of processing? Is a procedure available? [art. 19]		
The right of data portability is guaranteed [art. 20]		
The right to object to a processing is guaranteed [art. 21]		
The right to object to a decision based solely on automated processing including profiling (if applicable) [art. 22]		
Principles of data protection by design and data protection by default are applied [art. 25]		
An agreement with eventual joint controllers is established [art.26]		
The processor has been appointed and provides guarantees to implement appropriate technical and organisational measures and ensure the protection of the rights of the data subjects [art. 28]		
Anybody in charge of the processing is acting under instructions of the controller [art. 29]		
Records of processing activities are provided [art. 30]		

Security measures have been adopted [art. 32]		
Procedures have been adopted for dealing with data breaches and notification of breaches to DPA or to the affected individuals (if applicable) [art. 33 and 34]		
A pre-existing Data Protection Impact Assessment had already been done [art. 35]		
A Prior Consultation already took place [art. 36]		
A DPO has been appointed [art. 37]		
Data Controller or Data Processor abides to a Code of Conduct [art. 40]		
Data Controller or Data processor has received certification [art. 42]		
Transfer of Personal Data outside the EU is performed accordingly to the GDPR provisions [art. 44-49]		

Annex II – List of Possible Controls

No	Name of a Control	Control's Objective
1.	**Managing contracts between Data Controllers and Data Processors**	to reduce the risks associated with missing or incorrect contractual Data Protection clauses
2.	**Managing third parties with legitimate access to Personal Data**	to reduce the risk that legitimate access to Personal Data by third parties may pose to the data subjects' rights and freedoms.
3.	**Monitoring logical access controls**	to limit the risks that unauthorized persons will access Personal Data electronically.
4.	**Partitioning Personal Data**	to reduce the possibility that Personal Data can be correlated and that a breach of all Personal Data may occur.
5.	**Encrypting Personal Data**	to make Personal Data unintelligible to anyone without access authorization.
6.	**Anonymizing Personal Data**	to remove identifying characteristics from Personal Data.
7.	**Protecting Personal Data archives**	to define all procedures for preserving and managing the electronic archives containing the Personal Data.
8.	**Managing Personal Data violations**	to have an operational organisation that can detect and treat incidents that may affect the data subjects' civil liberties and privacy.
9.	**Tracing the activity on the IT system**	to allow early detection of incidents involving Personal Data and to have information that can be used to analyse them or provide proof in connection with investigations.
10.	**Combating malicious codes**	to protect access to public (Internet) and uncontrolled (partner) networks, workstations and servers from malicious codes that could affect the security of Personal Data.
11.	**Reducing software vulnerabilities**	to reduce the possibility to exploit software properties (operating systems, business applications, database management systems, office suites, protocols, configurations, etc.) to adversely affect Personal Data.
12.	**Reducing hardware vulnerabilities**	to reduce the possibility to exploit hardware properties (servers, desktop computers, laptops, devices, communications relays, removable storage devices, etc.) to adversely affect Personal Data.
13.	**Reducing the vulnerabilities of computer communications networks**	to reduce the possibility to exploit communications networks properties (wired networks, Wi-Fi, radio waves, fibre optics, etc.) to adversely affect Personal Data.
14.	**Reducing the vulnerabilities of paper documents**	to reduce the possibility to exploit paper documents properties to adversely affect Personal Data.
15.	**Reducing vulnerabilities related to the circulation of paper documents**	to reduce the possibility to exploit paper document circulation properties (within an

		organisation, delivery by vehicle, mail delivery, etc.) to adversely affect Personal Data.
16.	**Create procedures to address CoT and CoS**	To ensure that after such a change, no Personal Data is available
17.	**Permitting the exercise of the right to object**	to ensure that individuals have an opportunity to object to the use of their Personal Data.
18.	**Monitoring the integrity of Personal Data**	to be warned in the event of an unwanted modification or disappearance of Personal Data.
19.	**Reducing the vulnerabilities of individuals**	to reduce the possibility to exploit people (employees, individuals who are not part of an organisation but are under its responsibility, etc.) by adversely affecting Personal Data.
20.	**No collection of identifiable information, only pseudonyms, or anonym data**	to prevent identification of the data subject through collected data.
21.	**Active measure to preclude the use of particular data-items in the making of particular decisions**	to ensure that decisions are made based only on due data-items.
22.	**Limits on the use of information for a very specific purpose, with strong legal, organisational and technical safeguards preventing its application to any other purpose**	to ensure that information is used for the specified purpose and for nothing more than that.
23.	**Active measures to preclude the disclosure of particular data-items**	to ensure that only required and permitted data-items are disclosed.
24.	**Minimisation of Personal Data retention by destroying it as soon as the transaction for which it is needed is completed**	to ensure compliance with legislation and to prevent misuse of Personal Data.
25.	**Destruction schedules for personal information**	to ensure compliance with legislation and to prevent misuse of Personal Data.
26.	**Use of mathematical methods without collecting and registration source data to reach goals**	to avoid collection of non-authorized data without prejudice to reach goals.
27.	**Give the individual control over his or her data, for example by a secured website portal**	to ensure that the individual has control over his or her data according to his rights and responsibilities.
28.	**Introduction automated controls on the data quality**	to ensure that data quality is monitored and maintained on a regular basis.
29.	**Design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers**	to ensure that clients have a way of communicating their requests and complaints and to ensure that these are timely and adequately addressed.
30.	**Audit**	a generic control to ensure that all implemented Controls are in place

Annex III – Threat Taxonomy

The threat taxonomy provides descriptions of the threats in each category and examples to link them to the energy industry context. Each threat can also jeopardize the different security dimensions of confidentiality, integrity and availability.

Threats affecting primary assets

Threat Category	Threat	Explanation of threat	Specific Energy industry examples of Supporting Asset vulnerabilities	Questions for guidance	Proposed mitigation strategies
Illegitimate processing of Personal Data	No lawfulness of processing	To process Personal Data it is necessary to have a legal basis defined in Art.6 GDPR or the national Data Protection laws (e.g. consent of the data subject, contract with the data subject, documented legitimate interest of the Data Controller, legal requirements)		Is there a documented legal basis defined for the lawfulness of Data Processing?	Defining a legal basis for the process and controlling if the process follows that legal basis
Illegitimate processing of Personal Data	Collection exceeding purpose	More Personal Data is collected than what is necessary to achieve a specified purpose.	Collecting more detailed load profile data for the purpose of monthly billing, where much less detailed data would be sufficient to achieve the same objective.	1. What Personal Data do you need to collect for the purpose? 2. Is the collected data proportional to the purpose?	Minimizing the amount of Personal Data. Active measure to preclude the use of particular data-items in the making of particular decisions Limits on the use of information for a very specific purpose, with strong legal, organisational and technical safeguards preventing its application for any other purpose

Illegitimate processing of Personal Data	Unclear responsibilities for Data Processing.	It is not clear to data subjects what parties are involved in the processing of data and their respective roles.	(1) Installation organisation is acting as a subcontractor for the metering operator and is collecting data for the grid operator. (2) The energy service company (ESCo) hires a third party to collect data to provide energy saving advice to the consumer.	1. Are responsibilities clearly described and carried out for all parties? 2. Is responsibility for Data Processing part of a sub-contractors contract?	Informing data subjects Make a privacy policy, code of conduct or certify the processing of the data to be more transparent
Illegitimate processing of Personal Data	The protection of data is compromised outside the European Economic Area (EEA).	There is a risk that smart metering data may be at risk if sent outside of the EEA. Another risk is that Personal Data like metering data gives inside information about vital infrastructures in an unknown, maybe untruthful environment	Data Protection standards outside the EEA may not be secure and robust as those countries are not subject to the obligations within the GDPR. Foreign organisations use information about vital infrastructures and personal information to investigate people of interest.	1. Do you transfer the Personal Data outside the EEA? 2. To which country outside the EEA is the Personal Data transferred to? 3. Is the Personal Data transferred to a country that provides an adequate level of protection according to article 32 of GDPR? 4. How did you guarantee the protection of the Personal Data when transferred outside EEA? 5. Are all parties involved in implementation and operation established in the EU?	Anonymizing Personal Data Limiting Personal Data transfer to countries that provide an adequate level of protection according to the article 32 of the GDPR Active measures to preclude the disclosure of particular data-items Not transferring the source data, but only the outcomes

Inadequate information of the data subject	Incomplete information	The information provided to the data subject on the purpose and use of data is not complete	Information provided to consumers only consists of usage data, information about other information (such as the ability to detect communication disruptions) gathered is not provided.	1. How did you notify the purpose of the processing operation of Personal Data to the consumers?	Informing data subjects Clear and consistent communication of purpose and goals of data collection
Violation of the data subject's rights	Inability to execute individual rights (inspection rights)	If data are going to be held by multiple Data Controllers, then consumers should have a means by which to access these data from multiple sources using a single subject access request.	Petrol station and organisation providing invoices work together to enable charging of vehicles in joint controllership. Individuals should be provided with easy means to get insight in the data collected (e.g. by a unified user access right).	1. Is a procedure in place to easily inform consumers about the use of his Personal Data?	Informing data subjects Obtaining the consent of data subjects Giving the individual control over his or her data, for example by a secured website portal
Violation of the data subject's rights	Prevention of objections	Data subjects have the right to object to the processing of data. If they want to execute this right it must be (technically) possible.	Consumers cannot opt out to reading of detailed energy load profiles because read-out schemes are not configurable: There are no technical or operational means to allow compliance with a data subject's objection.	1. Is it possible to change the collection of Personal Data in the Smart Grid Use Case after the consumer's objection? 2. Can consumers object to processing of Personal Data use by certain technologies?	Permitting the exercise of the right to object Make a privacy policy, code of conduct or certify the processing of the data to be more transparent

Violation of the data subject's rights	A lack of transparency for automated individual decisions	Automated processing of Personal Data intended to evaluate certain personal aspects or conduct is used but the data subjects are not informed about the logic of the decision-making.	Remote disconnection is performed without providing clear explanation of the reasons to the user.	1. Are consumers informed of automated information processing? 2. How are the consumers notified of automated individual decisions?	Informing data subjects
Violation of the data subject's rights	Lack of correction of Personal Data	There is no way for the data subject to initiate a correction of his data according to article 16 of the GDPR. The Data Controller and / or Data Processor are not sufficiently prepared to respond to such requests.	A personalized overview of Personal Data from the data subject cannot be corrected from the database that holds the data.	1. Are there processes to meet the consumer's rights on data collection, access, deletion and correction? 2. Are you able to provide overview of data collected? 5. Are you able to correct the data on request?	Permitting the exercise of the direct access right Allowing the exercise of the right to correct according to article 16 of the GDPR Design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers Give the individual control over his or her data, for example by a secured website portal
Violation of the data subject's rights	Lack of erasure of Personal Data	There is no way for the data subject to initiate an erasure of his data according to article 17 of the GDPR. The Data Controller and / or Data Processor are not sufficiently prepared to respond to such requests.	A personalized overview of Personal Data from the data subject cannot be erased from the database that holds the data.	1. Are there processes to meet the consumer's rights on data collection, access, deletion and correction? 2. Are you able to provide overview of data collected? 5. Are you able to delete the data on request?	Permitting the exercise of the direct access right Allowing the exercise of the right to erase (right to be forgotten) according to article 17 of the GDPR Design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers Give the individual control over his data, for example by a secured website portal

Compliance violations in the contracts	Missing or incorrect contractual Data Protection clause	It is required to have a Data Protection clause in contracts for Data Processing on behalf. The content of the Data Protection clause is legally required and different in the EU countries. There are additional requirements for Data Processors in third Countries.	To provide consumption data to the customers by internet platforms IT-provider gets into contact with these data as a Data Processor.	Are there Data Protection clauses and technical and organizational measures defined in the contract with the provider involved in the process?	Implementation of Data Protection clauses for Data Processing on behalf together with the procurement department
Personal Data integrity loss	Lack of quality of data for the purpose of use	If data is used for certain processes it should be adequate.	For billing on a daily basis data should be registered on a daily basis. For disconnecting electricity supply the exact location (address) and reasons should be conclusive. Based upon wrong consumption data a wrong invoice is sent. A comma is used as a separator where a full-stop is intended. This leads to wrong invoice.	1. Are automated input validation and reconciliation controls implemented? 2. How do you ensure data quality for the purpose of use? 3. Are there test procedures for data quality?	Monitoring the integrity of Personal Data Introduction of automated controls on the data quality
Personal Data integrity loss	Inability to respond to requests for subject access, correction or deletion of data in a timely and satisfying manner.	The data is distributed across several business units and an integrated overview cannot be made within a short time frame.	Metering data is stored and maintained by the technical department, reactions on commercial offers are stored at the commercial department, questions and answers are stored at the	1. Are there processes to meet the consumer's rights on data collection, access, deletion and correction? 2. Are you able to provide overview of data collected? 3. Are you able to provide what	Allowing the exercise of the right to correct Design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers Give the individual control over his or her data, for example by a secured website

			service department. Combining this data in one overview takes (a lot of) effort.	data is transferred to a third party? 4. Can an overview of what data is provided to whom be provided? 5. Are you able to delete the data on request?	portal
Damage to individual	Discrimination				
Damage to individual	Identify Theft or Fraud				
Damage to individual	Financial loss				

Damage to individual	Other significant economic or social disadvantage				

Threats affecting Supporting Assets

Threat Category	Threat	C	I	A	Explanation of threat	Specific Energy industry examples of Supporting Asset vulnerabilities	Questions for guidance
Physical attack (deliberate/ intentional)	Fraud	X	X		Fraud committed by humans. I.e. Forgery of paper documents	Forgery is only possible in an environment where RBAC does not exist and people get much too much access rights. In a controlled environment where need to know and need to do is normal, this can't be a problem. Falsifiable information can lead to unreliable consumer and metering information	1. Is Identity and Access Management in place (e.g. Role Based Access Control)? 2. For critical information change, is separation of duties in place?
Physical attack (deliberate/ intentional)	Sabotage		X	X	Intentional actions (non-fulfilment or defective fulfilment of personal duties) aimed to cause disruption or damage to IT assets		
Physical attack (deliberate/ intentional)	Vandalism		X	X	Act of physically damaging IT assets		
Physical attack (deliberate/ intentional)	Theft (of devices, storage media and documents)	X	X	X	Stealing information or IT assets. Robbery. I.e. theft of a laptop from a hotel room; theft of a professional mobile phone by a pickpocket; retrieval of a discarded storage	Every device which contains sensitive data about the Smart Grid environment will cause to unacceptable risk of alteration and abuse of those data. When information is	1. Are hardware devices containing data protected against abuse? (password, Pin code, biometrical recognition,

					device or hardware; loss of an electronic storage device.	retrieved about brand and type of firewalls, IP-ranges, OS and SCADA-system brand and type, a serious attack is made easy.	pattern recognition) 2. Is the data in the hardware encrypted?
Physical attack (deliberate/ intentional)	Information leak /sharing	X			Sharing information with unauthorized entities. Loss of information confidentiality due to intentional human actions (e.g., information leak may occur due to loss of paper copies of confidential information).	Paper documents with personal (metering, billing) information of the consumers are not security stored and therefore accessible to unauthorized persons.	1. Are measures taken to prevent unauthorized access to paper documents with Personal Data? 2. Is printing on demand installed? 3. Are there secure lockers available to store printed data?
Physical attack (deliberate/ intentional)	Unauthorized physical access / Unauthorized entry to premises	X			Unapproved access to facility		
Physical attack (deliberate/ intentional)	Coercion, extortion or corruption	X	X	X	Actions following acts of coercion, extortion or corruption		
Physical attack (deliberate/ intentional)	Damage from the warfare	X	X	X	Threats of direct impact of warfare activities		
Physical attack (deliberate/ intentional)	Terrorist attack	X	X	X	Threats from terrorists		

Unintentional damage / loss of information or IT assets	Information leak /sharing due to human error	X			Information leak / sharing caused by humans, due to their mistakes or working conditions. I.e. high workload, stress or negative changes in working conditions; assignment of staff to tasks beyond their abilities; poor use of skills, etc.	When maintenance people are not skilled to do their job, there is high risk of unnoticed security breaches. You can't expect that stressed and unskilled maintenance people are able to recognize security events/incidents where high skilled expertise is necessary. They will recognize a security breach when systems are already going down, this is too late!!	1. Are employees adequately trained to do their job? 2. Is the workload acceptable? 3. Are employees trained to recognize security breached and vulnerabilities which can lead to a security breach?
Unintentional damage / loss of information or IT assets	Erroneous use or administration of devices and systems	X	X	X	Information leak / sharing / damage caused by misuse of IT assets (lack of awareness of application features) or wrong / improper IT assets configuration or management.		
Unintentional damage / loss of information or IT assets	Using information from an unreliable source	X	X	X	Bad decisions based on unreliable sources of information or unchecked information.		
Unintentional damage / loss of information or IT assets	Unintentional change of data in an information system		X		Loss of information integrity due to human error (information system user mistake).		

Unintentional damage / loss of information or IT assets	Inadequate design and planning or improper adaptation	X	X	X	Threats caused by improper IT assets or business processes design (inadequate specifications of IT products, inadequate usability, insecure interfaces, policy/procedure flows, design errors). I.e. ihe implemented logging mechanism is insufficient. It does not log administrative processes.	It is not logged who has accessed the meter load profile. In a smart meter/ smart energy system it is not known which entity reads, collects, writes, changes or deletes data. After an incident, or just for routine checks, it is necessary to have	1. What are the security controls to take non-repudiation into account? 2. How is the access to the Personal Data being logged?
Unintentional damage / loss of information or IT assets	Damage caused by a third party	X	X	X	Threats of damage to IT assets caused by third party.		
Unintentional damage / loss of information or IT assets	Damages resulting from penetration testing	X	X	X	Threats to information systems caused by conducting IT penetration tests inappropriately.		
Unintentional damage / loss of information or IT assets	Loss of information in the cloud	X	X	X	Threats of losing information or data stored in the cloud.		
Unintentional damage / loss of information or IT assets	Loss of (integrity of) sensitive information		X		Threats of losing information or data, or changing information classified as sensitive.		

Unintentional damage / loss of information or IT assets	Loss of devices, storage media and documents	X		X	Threats of unavailability (losing) of IT assets and documents.	Every device which contains sensitive data about the Smart Grid environment will cause to unacceptable risk of alteration and abuse of those data. When information is retrieved about brand and type of firewalls, IP-ranges, OS and SCADA-system brand and type, a serious attack is made easy	1. Are hardware devices containing data protected against abuse? (password, Pin code, biometrical recognition, pattern recognition) 2. Is the data in the hardware encrypted?
Unintentional damage / loss of information or IT assets	Destruction of records			X	Threats of unavailability (destruction) of data and records (information) stored in devices and storage media.		
Disaster (natural, environmental)	Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy snowfalls, heavy winds)			X	Threats of damage to information assets caused by natural or environmental factors.		
Disaster (natural, environmental)	Fire			X			
Disaster (natural, environmental)	Pollution, dust, corrosion			X			
Disaster (natural, environmental)	Thunder strike			X			
Disaster (natural,	Water			X			

environmental)							
Disaster (natural, environmental)	Explosion			X			
Disaster (natural, environmental)	Dangerous radiation leak			X			
Disaster (natural, environmental)	Unfavorable climatic conditions			X			
Disaster (natural, environmental)	Threats from space / Electromagnetic storm		X	X			
Disaster (natural, environmental)	Wildlife			X			
Failures/ Malfunction	Failure of devices or systems	X	X	X	Threat of failure/malfunction of IT supporting infrastructure (i.e. degradation of quality, improper working parameters, jamming). The cause of a failure is mostly an internal issue		
Failures/ Malfunction	Failure or disruption of communication links (communication networks)			X	Threat of failure or malfunction of communications links.		

Failures/ Malfunction	Failure or disruption of main supply			X	Threat of failure or disruption of supply required for information systems. I.e. Loss of power can harm hardware and software and lead to unavailability of computing systems, network equipment and disruption of Smart Grid devices	Due to power loss crash of hard drives or other hardware components; Due to power loss crash of OS or loss of unsaved data; Long time power loss has impact on availability of systems. Not all systems will be covered by emergency power equipment; Very long time loss of power will lead to disruption in refuelling emergency power and lack of emergency power	1. Are measures taken to avoid disruption of power, such as UPS and no-break? 2. For vital information systems are uninterruptible power supplies in place? 3. Are there provisions made in order to refuel in time?
Failures/ Malfunction	Failure or disruption of service providers (supply chain)			X	Threat of failure or disruption of third party services required for proper operation of information systems.		
Failures/ Malfunction	Malfunction of equipment (devices or systems)	X	X	X	Threat of malfunction of IT hardware and/or software assets or its parts. I.e. Errors during updates, configuration or maintenance; replacement of components, etc.	Changing of smart meter software can lead to changes of metering data which will damage the integrity of the consumption profile. This can affect the billing process and may cause reputation damage for the grid operator.	1. Is configuration management in place? 2. Is patch management in place? 3. Are software updates tested in a test environment, before use in the operational environment? 4. Are source code reviewed,

							when software is custom or customized for a specific system?
Outages	Absence of personnel			X	Unavailability of key personnel and their competences.		
Outages	Strike			X	Unavailability of staff due to a strike		
Outages	Loss of support services			X	Unavailability of support services required for proper operation of the information system.		
Outages	Internet outage			X	Unavailability of the Internet connection.		
Outages	Network outage			X	Unavailability of communication links		
Eavesdropping/ Interception/ Hijacking	War driving	X	X	X	Threat of locating and possibly exploiting connection to the wireless network.		
Eavesdropping/ Interception/ Hijacking	Intercepting compromising emissions	X			Threat of disclosure of transmitted information using interception and analysis of compromising emission.		

Eavesdropping/ Interception/ Hijacking	Interception of information	X			Threat of interception of information that is improperly secured in transmission or by improper actions of staff. I.e. watching a person's screen without them knowing while on the train; taking a photo of a screen; geo-location of hardware; remote detection of electromagnetic signals, shoulder-surfing etc.	Where copper wiring is still in use, it is possible to listen to the signals on the communication lines. This makes it possible to interpret and reuse signals send over the communications network. Other example, metering operators talking about personal Information from consumers in their meetings or public areas.	1. Is copper to FO replacement part of the planning? 2. Are screen savers in use to make it impossible to look on the screen or take pictures of the screen? 3. Any measures taken to protect the data when using public wireless network? 4. Are remote access controls disabled in an unprotected area (e.g. WiFi, Bluetooth, infrared)? 6. Is an awareness campaign taking place? 7. Are incidents shared to learn from them?
Eavesdropping/ Interception/ Hijacking	Interfering radiation			X	Threat of failure of IT hardware or transmission connection due to electromagnetic induction or electromagnetic radiation emitted by an outside source.		

Eavesdropping/ Interception/ Hijacking	Replay of messages			X	Threat in which valid data transmission is maliciously or fraudulently repeated or delayed.		
Eavesdropping/ Interception/ Hijacking	Network Reconnaissance, Network traffic manipulation and Information gathering	X	X		Threat of identifying information about a network to find security weaknesses.		
Eavesdropping/ Interception/ Hijacking	Man in the middle/ Session hijacking	X	X	X	Threats that relay or alter communication between two parties. I.e. interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc.	Observation of metering and technical data between the smart meters and the central system with a false GSM base station by unauthorized person.	1. Are measure taken to prevent interception? (like Man-in-the-middle-attack) 2. Is time-stamping in place? 3. Is authentication and authorisation in place to refuse unknown devices? 4. Is the (wireless) connection
Nefarious Activity/ Abuse	Identity theft (Identity Fraud/ Account)	X	X	X	Threat of identity theft action.		
Nefarious Activity/ Abuse	Receiving unsolicited E-mail			X	Threat of receiving unsolicited email which affects information security and efficiency		

Nefarious Activity/ Abuse	Denial of service			X	Threat of service unavailability due to massive requests for services.	DDoS attacks can lead to unavailability. Consumers cannot reach websites of supplier. Smart Grid components cannot communicate which lead to disruption of the self-healing opportunities of the grid.	1. Are attack scenarios investigated and known? 2. Are mitigating measures in place to detect and stop a D(D)oS attack? 3. Is a Disaster Recovery plan in place to recover as soon as possible after a successful attack?
Nefarious Activity/ Abuse	Malicious code/ software/ activity	X	X	X	Threat of malicious code or software execution. I.e. Software Key-logger logs all keystrokes and/or Trojan sends commands and data to attacker's computer system	Allows attackers to engineer and reuse usernames, passwords, compromising data to be observed and searched for specific words, sentences etc.	1. Are all computer systems equipped with anti-virus, anti-malware solutions? (if available for the particular OS) 2. Are anti-malware and anti-virus solutions updated on daily basis? 3. Is anti-virus set so that the full computer scans on a regular basis?
Nefarious Activity/ Abuse	Social Engineering			X	Threat of social engineering type attacks (target: manipulation of personnel behaviour).		
Nefarious Activity/ Abuse	Information Leakage	X			Threat of leaking important information.		
Nefarious Activity/	Generation and use of	X	X		Threat of use of rogue		

Abuse	rogue certificates				certificates.		
Nefarious Activity/ Abuse	Manipulation of hardware and software	X	X	X	Threat of unauthorised manipulation of hardware and software. I.e: Use of USB flash drives or disks that are ill-suited to the sensitivity of the information; use or transportation of sensitive hardware for personal purposes, etc.	The use of uncontrolled hardware can introduce viruses in a normally clean environment. Energy companies which think they are secured against Internet threats, become vulnerable from unexpected malware. 2nd: the use of hardware, which is not secure by Energy companies, can cause serious risks (not able to mitigate DDoS attacks, the use of hard coded high privileged accounts with the use of simple username/password, not able to use VPN connections etc.).	1. Are unknown devices accepted to use in the IT/OT environment? 2. Are anti-virus and anti-malware measures present on all I/O-ports? 3. Are crucial systems protected against the use of unknown storage devices (e.g. USB-devices)?
Nefarious Activity/ Abuse	Manipulation of information		X		Threat of intentional data manipulation to mislead information systems or somebody or to cover other nefarious activities		
Nefarious Activity/ Abuse	Misuse of audit tools	X	X	X	Threat of nefarious actions performed using audit tools (discovery of security weaknesses in information systems).		

Nefarious Activity/ Abuse	Misuse of information/ information systems	X	X	X	Threat of nefarious action due to misuse of information systems. I.e. addition of incompatible hardware resulting in malfunctions; changing of components essential to the owner operation of an application, etc.	Changing of smart meter hardware can lead to changes of metering data which will damage the integrity of the consumption profile. This can affect the billing process and may cause reputation damage for the grid operator.	1. Is change of hardware components present? 2. Are measures in place to detect alteration in hardware in critical (smart energy) devices? 3. Are these measures able to generate an alarm when a device is accessed or modified?
Nefarious Activity/ Abuse	Unauthorized activities	X	X	X	Threat of nefarious action due to unauthorised activities. I.e. Installation of Key-loggers; key-logger logs all keystrokes. Allows attackers to reuse usernames, passwords, compromising data to be observed and searched for specific words, sentences etc.	Hardware key-loggers can be used to collect data like usernames and passwords, commands, etc. This will make it possible to login in the SCADA system and use a dispatcher's role to communicate with the SCADA system.	Are keyboard connectors, USB-ports and other I/O ports checked for unknown hardware devices on regular bases?
Nefarious Activity/ Abuse	Unauthorized installation of software	X	X	X	Threat of unauthorised installation of software.		

Nefarious Activity/ Abuse	Compromising confidential information	X			Unauthorized parties obtain access to personal information by breach of security or lack of security implementation.	(1) Load profile not end-to-end encrypted and could be read & processed by unauthorized third party, e.g. a network provider. (2) A faulty implementation of security mechanisms (locally or on a centralized server) enables hackers to access a memory area containing identifiable meter load profile history.	1. Is an information security policy described, implemented and in place? 2. Have the information security controls been audited? Checked by an auditor? 3. Did you perform a penetration test after implementation of the security controls? 4. How is the incident response management and the intrusion detection system implemented according to international standards?
Nefarious Activity/ Abuse	Hoax			X	Threat of loss of IT assets security due to cheating.		
Nefarious Activity/ Abuse	Remote activity (execution)	X	X	X	Threat of nefarious action by attacker remote activity		

Nefarious Activity/ Abuse	Targeted attacks (APTs etc.)	X	X	X	Threat of sophisticated, targeted attack which combine many attack techniques. I.e. malwares that log all keystrokes and/or that sends commands and data to attacker's computer system	Allows attackers to engineer and reuse usernames, passwords, compromising data to be observed and searched for specific words, sentences etc.	1. Are all computer systems equipped with anti-virus, anti-malware solutions? (if available for the particular OS) 2. Are anti-malware and anti-virus solutions updated on daily basis? 3. Is anti-virus set so that the full computer scans on a regular basis?
Nefarious Activity/ Abuse	Failed business process			X	Threat of damage or loss of IT assets due to improperly executed business process.		
Nefarious Activity/ Abuse	Brute force	X			Threat of unauthorised access via systematically checking all possible keys or passwords until the correct one is found.		

Nefarious Activity/ Abuse	Abuse of authorizations	X	X		Threat of using authorised access to perform illegitimate actions. I.e. content scanning; illegitimate cross-referencing of data; raising of privileges, wiping of usage tracks; sending of spam via an e-mail program; misuse of network functions; Access rights are not revoked when they are no longer necessary.	(1) After a change of supply the former supplier has still valid access credentials to (historic) read out meter data. (2) After moving house, the new tenant has access to historic readings in the meter. (3) Employees who change job positions are still authorized to access data, not necessary for their new job. (4) Meter operators have the privilege to make data accessible for viewing or manipulation (deletion, modification, movement, etc.).	1. Is change of data authorized by a change management process? 2. Are dedicated devices in use to change software function, to avoid unwanted introduction of viruses or malware? 3. Did you implement an access control policy? 4. Who has access to the Personal Data? 5. Does your access control policy covers all persons involved in processing Personal Data? 6. How do you deal with access control rights when staff leave the organisation? 7. Do you have a regular review of the access control policy?

Bibliography

1. European Commission. Smart Grid Mandate. Brussels: European Commission, 2011.
2. Workgroup on Smart Grid Information Security. SGCG - WG Smart Grid Information Security report. 2011.
3. European Union (EU) General Data Protection Regulation, Regulation (EU) 2016/679
4. ISO International Standard, Information technology - Security techniques - Information security management, ISO/IEC 27005:2011
5. ISO 31000
6. ENISA Threat Taxonomy, version 1.0, 2015
7. 2014/724/EU: Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems
8. The Commission Recommendation 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart metering systems
9. Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, revised and adopted on 4 October 2017
10. Article 29 Working Party Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (‘DPIA Template’) prepared by Expert Group 2 of the Commission’s Smart Grid Task Force
11. Article 29 Working Party Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (‘DPIA Template’) prepared by Expert Group 2 of the Commission’s Smart Grid Task Force