SYNCHRONICITY

GA no:	732240
Action full title:	SynchroniCity: Delivering an IoT enabled Digital Single Market for Europe and Beyond
Call/Topic:	Large Scale Pilots
Type of action:	Innovation Action (IA)
Starting date of action:	01.01.2017
Project duration:	33 months
Project end date:	30.09.2019
Deliverable number:	D1.4
Deliverable title:	Privacy by design methodology & PIA
Document version:	1.0
WP number:	WP1
Lead beneficiary:	Mandat International (MI)
Main author(s):	Lucio Scudiero, Sebastien Ziegler
Internal reviewers:	Alex Gluhak, Herby Hulsebos, Adrian Slatcher, Francesca Spagnoli
Type of deliverable:	Report
Dissemination level:	Public
Delivery date from Annex 1:	M5
Actual delivery date:	M5 (30.05.2017)

This deliverable has been written in the context of a Horizon 2020 European research project, which is co-funded by the European Commission. The opinions expressed and arguments employed do not engage the supporting parties.

Executive Summary

This report constitutes deliverable no. 1.4 (Privacy by design methodology & PIA) of the SYNCHRONICITY project. The report has been prepared by Lucio Scudiero with the contribution of Sébastien Ziegler.

The document is developed to provide the stakeholders within the project, starting from the Cities, with a privacy by design and by default methodology, to be applied throughout the different phases of the project itself, and a Privacy Impact Assessment framework, which is in itself part and parcel of such a methodology.

The document starts with a set of abbreviations and definitions; section 1 introduces the scope of the document, the relevant European legal framework and the main features of the approach encapsulated in the formula “privacy by design and by default”. Section 2 provides some privacy by design guidelines to smart cities, whereas in Section 3 the PIA methodology is explained; the elements of the PIA are then detailed in Sections 4 and 5 in the form of different dedicated checklists aimed at mapping the crucial aspects of the personal data processing; in Section 5 a strategy for the involvement of the citizens in the assessment is suggested, whereas Section 6 contains the matrixes whereby risks can be identified and countermeasures applied. Section 7 explains how and to whom the PIA’s results should be reported. Conclusive remarks and recommendations are exposed in Section 8. The Annex is a collection of the relevant questions and matrix developed to measure and tackle the risks.

Abbreviations and definitions:

Component (of a Smart City) = any item, object, process, sensor or thing used within the smart city's initiative under assessment which is linked to and/or is used in connection with personal data processing**.**

Data Controller = the 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.

Data Processor = a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Subject = an identified or identifiable natural person.

Directive = 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.

ePD = ePrivacy Directive, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC.

GDPR = General Data Protection Regulation, Regulation EU/679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

IoT = Internet of Things.

LSP = Large-scale Pilot.

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, particularly 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.

Personal data breach = a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

PIA (Privacy Impact Assessment) = a process whereby a conscious and systematic effort is made to assess privacy risks to individuals in the collection, use and disclosure of their personal data. PIAs help identifying privacy risks, foresee problems and bring forward solutions. In this document, the term PIA equates to Data Protection Impact Assessment (DPIA).

Prior Informed Consent = any freely given, specific, informed and unambiguous indication of the data subject's 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, before the actual processing of personal data takes place.

PbD = Privacy by Design and by Default, a principle of the GDPR according to which the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. The controller shall also implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons (hereinafter “PbD”).

Purpose limitation = an overarching privacy principle, according to which personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Special categories of data = data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data and 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.

ToE = Target of Evaluation, the object of the PIA **(**see *infra* paragraph 3 (1) let. a.)

WP = Work Package.

WP29 = Article 29 Working Party, the group of European Data Protection Authorities entrusted by

Article 29 of the Directive with consultative powers, which has the task to issue opinions and recommendations on all matters relating to the protection of persons with regard to the processing of personal data.

Table of Content

List of figures

1 INTRODUCTION

As privacy concerns spread through society, the interest in PIA increases, in that it is a pivotal tool in the perspective of filling the information asymmetry between data controllers and data subjects, by putting the former under the obligation to design, from the start of development, processing operations which are not detrimental to society's and individuals' liberty.

A PIA is a methodology designed to describe the processing, assess the necessity and proportionality of it and to help manage the risks to the rights and freedoms of natural persons resulting thereby (by assessing them and determining the measures to address them). It is intended as an important accountability tool, as it not only fosters the compliance of data controllers with the obligations set by the applicable data protection law, but also to demonstrate that appropriate measures have been taken to ensure compliance with it.

To date, different methodologies for PIAs exist at a general level, whereas the European data protection authorities, in a recently issued document, have called to develop specific ones for specific sectors, such as smart cities.[1] One of the turning points in PIA development in Europe, due to its scale and complexity, was the endorsement of the European Union's (EU) Radio-Frequency Identification (RFID) PIA framework by the Article 29 Working Party in February 2011.[2] This experience was then followed by a data protection impact assessment (DPIA) framework developed for smart metering systems.[3] The next and ultimate turning point has been the approval of Regulation 679/2016 on the protection of personal data, whose Article 35 explicitly provides for a PIA, in the terms that will be extensively explained in this document.

a. The European legal framework

Privacy and data protection have always been crucial issues at European level.

The first key norm in the European Legal Framework is Article 8 of the European Convention on Human Rights (hereinafter "*ECHR"*). It sets out the right to respect for private and family life, making clear that those rights are not absolute, because public authorities can interfere with them

[1] 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".
[2] Privacy and Data Protection Impact Assessment Framework for RFID Applications Brussels, 12 January 2011. Available at http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf.
[3] European Commission, "*DPIA Template for Smart Grid and Smart Metering Systems"*. Available at http://ec.europa.eu/energy/en/content/dpia-template-smart-grid-and-smart-metering-systems.

in certain circumstances.

When the Council of Europe (CoE) adopted its *Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Council of Europe, 1981), it merged data protection and privacy in a single provision: "*The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")*" (Article 1, *Convention n.108*).[4] The Convention is currently under revision.[5]

Through the Charter of Fundamental Rights of the European Union (hereinafter "*CFREU")* and the *Treaty establishing a Constitution for Europe* (2004), the European Union incorporated both privacy and data protection rules in its "constitutional" framework. Mirroring Article 8 of the ECHR, the Article 7 *CFREU* establishes the right of everyone "*to respect for his or her private and family life, home and communications*", while Article 8 *CFREU* specifically regulates "*Protection of personal data*". The two mentioned provisions thus make a distinction between privacy and data protection at the highest hierarchical level in EU law, as the CFREU is primary law and provides for principles against which the lawfulness of secondary law (e.g. Regulations and Directives) is checked. Article 8 *CFREU* establishes some high level criteria for the lawful processing of personal data, such as the reference to the fact that personal data shall be processed for "*specified purposes*", upon prior data subject's "*consent*" or "*some other legitimate basis laid down by law*". It also stipulates that "*Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*" and that "*an independent authority*" shall oversee the compliance with data protection rules.

The *Lisbon Treaty* [6] (2007) states that the EU has its foundations in the amended *Treaty on the European Union (TEU)* [7] and the *Treaty on the Functioning of the European Union (TFEU)*[8], which, together with the *CFREU,* complete the institutional and constitutional European legal framework, and in so doing they provide EU institutions with a legal basis to adopt data protection rules.

---

[4] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, 28.I.1981, in *www.coe.int*.

[5] For more information, see http://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet.

[6] *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community*, signed at Lisbon, 13 December 2007, in *eur-lex.europa.eu.*

[7] *Treaty on European Union and the Treaty on the Functioning of the European Union*, 2012/C 326/01, in *eur-lex.europa.eu.*

[8] Ibid.

Accordingly, Article 16 *TFEU* states that: "*Everyone has the right to the protection of personal data concerning them*. *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities* […]".

At a secondary[9] level in EU law, one legal act worth to mention is *Regulation 45/2001/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*[10]. It establishes data protection rules for EU Institutions.

However, the main EU legal instruments that regulate data protection in the EU are the *Data Protection Directive (95/46/EC)* and the *Privacy and Electronic Communications Directive (2002/58/EC, as amended by Directive 2009/136/EC)*.

The ***Data Protection Directive (95/46/EC)*** builds on the *Convention n.108*, and lays down a minimum set of data protection rules for all Member States of the European Union, which have implemented it through national laws. Some of the main points of the Directive are:

- **Data minimization,** meaning that the processing of personal data must be the least intrusive possible, and that only personal data that are necessary for the envisaged purposes shall be collected and processed;
- **Principle of data quality**: personal data must be "***relevant and not excessive*** *in relation to the purposes*". *They must also be* "*accurate and, where necessary,* ***kept up to date***" (Article 6);
- **Principle of transparency**: *"personal data must be processed fairly and lawfully"* and "*collected for* ***specified, explicit and legitimate purposes***" (Article 6);
- Principle of **legitimacy of data processing**: Personal data may be processed only if the data subject has unambiguously given his/her **explicit consent** or processing is necessary: for the

[9] With "secondary" EU law we refer to rules adopted pursuant the principles and rules on the production of Eu law set out by primary EU law, *ie* the Treaties and the CFREU.

[10] Regulation 45/2001/EC of the European Parliament and of the Council *on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*, in eur-lex.europa.eu.

performance of a contract to which the data subject is party or; for compliance with a legal obligation to which the controller is subject or; in order to protect the vital interests of the data subject or; for the performance of a task carried out in the public interest or; for the purposes of the legitimate interests pursued by the controller (Article 8);

- **Principle of information,** which must be given to the data subjects*:* the controller must provide the data subject from whom data are collected with certain information relating to himself/herself (**the identity of the controller, the purposes of the processing, recipients of the data, right of access/rectify the data concerning him/her, means of processing etc.**) (Article 10);
- **Special categories of data** (so-called "sensitive personal data"): data "*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership*" and "*health or sex life*" can only be processed in exceptional circumstances (Article 8);
- the data subject's **right of access to data**: every data subject should have the right to obtain from the controller "*without excessive delay or expense: confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed* […]" (Article 12);
- The **right to object to the processing of data**: the data subject should have the right to object, on legitimate grounds, to the processing of data relating to him/her (Article 14);
- The ***confidentiality and security of processing****:* any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, protecting them "*against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access* […]" (Articles 15 and 16);
- The **notification of processing** to a supervisory authority: the controller must notify the national supervisory authority before carrying out "*any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes"* (Article 18)*.*

Following Article 16 *TFEU*, which is the legal basis for the adoption of data protection rules in the

EU, the European Union legislator adopted the GDPR[11]. The aim of the GDPR is to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States.

The logic of the adoption of a GDPR was to prevent disparities between Member States in terms of procedures and sanctions, harmonizing the data protection in the EU. Its key principles and provisions for the IoT and smart cities landscape will be outlined below in paragraph 2.

The Data Protection Directive (and the GDPR alike) is complemented by ***Directive 2002/58/EC on privacy and electronic communications*** (ePrivacy Directive)**,** which concerns the processing of personal data and the protection of privacy in the electronic communications sector and states specific requirements concerning the protection of personal data and privacy of the users of electronic communication services. Key principles of Directive 2002/58/EC are outlined below in paragraph 2. It is noteworthy that the Directive is currently under revision; in fact, on 10 of January 2017 the European Commission published a proposal for an ePrivacy Regulation which is going to be discussed by the EU legislator and eventually to replace current rules for privacy in digital services.[12]

b. What is Privacy by Design

Privacy by design (hereinafter "PbD") is an approach to design and development of innovations where privacy is operationalized into requirements and part of the innovation through development. According to the European Data Protection Supervisor ("EDPS"), PbD requires the "*integration of data protection and privacy from the very inception of new products, services and procedures that entail the processing of personal data*".[13]

PbD therefore requires a translation of legal considerations into requirements through requirements engineering: '*Requirement engineering is concerned with the transformation of needs expressed in natural language into language that is precise enough to engineer systems*.'[14]

---

[11] COM/2012/011 final - 2012/0011 (COD), in *eur-lex.europa.eu.*

[12] For more background information, please check https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation#Article.

[13] Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union".

[14] Gürses, S., Troncoso, C. & Diaz, C., 2011. Engineering privacy by design. *Computers, Privacy & Data Protection*. Available at: https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf [Accessed September 9, 2013].

The concept of Privacy by Design was developed for the first time in the report "*Privacy-enhancing technologies: the path to anonymity*" published in 1995.[15]
This report was the result of a joint project set up by the Dutch Data Protection Authority and the Ontario Information Commissioner, respectively led by John Borking and Ann Cavoukian.

The approach developed in that report relies on seven foundation principles.

1. **Proactive not Reactive; Preventative not Remedial**

The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

2. **Privacy as the Default Setting**

Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data is automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

3. **Privacy Embedded into Design**

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. **Full Functionality — Positive-Sum, not Zero-Sum**

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security,

15 Privacy enhancing technologies: the path to anonymity [1995] PrivLac PRpr112. Available at http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf.

demonstrating that it is possible to have both.

5. End-to-End Security — Full Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. Visibility and Transparency — Keep it Open

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy — Keep it User-Centric

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

With the approval of the GDPR, this approach has been incorporated into EU law, what makes it binding and the lack thereof subject to sanctions.

It requires that the data controllers act in a proactive way; In fact, "*taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing*", they shall "*both at the time of the determination of the means for processing and at the time of the processing itself, implement* ***appropriate technical and organisational measures****, such as pseudonymisation, 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 this Regulation and protect the*

rights of data subjects".[16]

Not only products, or IT deployments, must be privacy-by-designed (by means of appropriate technical measures), but also processes, which require that organizational measures, appropriate to each case at stake, are also in place. The latter concept is clarified by Recital 78 of the GDPR, whereby a reference to the controller's "policies" is also made:
"(…) *the controller should adopt* ***internal policies*** *and implement measures which meet in particular the principles of data protection by design and data protection by default*".

An example of policies and measures is set out by the same Recital 78:

"*Such measures could consist, inter alia, of* ***minimising*** *the processing of personal data,* ***pseudonymising*** *personal data as soon as possible,* ***transparency*** *with regard to the functions and processing of personal data, enabling the* ***data subject to monitor the data*** *processing, enabling the controller to create and improve security features*".

Notably for smart cities, Recital 78 of the GDPR also recommends that
"*The principles of data protection by design and by default should also be taken into consideration in the context of* ***public tenders***". This is highly relevant for Synchronicity, as it foresees an open call phase for SMEs' experiments.

PRIVACY BY DESIGN AND BY DEFAULT IN THE OPEN CALLS

Safeguards recommended to cities running the **open calls**

- A **dedicated privacy policy** should be **embedded in the notice of call** (defining roles, communication of data, data retention, participants' privacy rights, consequences of participation/consent)
- A **helpdesk** should be kept open during the call period;
- **Participants' withdrawals and data protection rights should be enforced** during the open call period. This should include the enforcement of their right to be forgotten, as the case may be, after having performed the assessment prescribed by the Court of Justice of the European Union In case C-131-12.
- **Define the ethics/privacy criteria that should be taken into account during the evaluation phase**, such as:

[16] Article 25 of the GDPR.

- Clear and trustworthy identification of the privacy and other fundamental rights risks entailed by the proposal;
- Clear and sound remediation measures to the identified risks;
- Privacy by design and Privacy by default solutions;
- Effectiveness of security measures (protection against third parties' intrusion, anonymisation etc.)

- **Each element of the proposal (amongst which privacy) could have a weight which could be predetermined beforehand** in the notice of call itself (for example, privacy by design may account for 1 third of the overall total score attributed to a given proposal);
- **Criteria to evaluate procedures for the enforcement of data subjects' rights** (priority could be given to innovative/user-centric solutions, such as dashboards and control panels, push up alerts to data subjects of «extraordinary» processing of data)
- Draft a clause that clearly mandates the participants to **identify the legal basis** on which data processing take place.

In addition to the foregoing, it is worth to recall that through various opinions,[17] the EDPS has provided some guidance on PbD.

According to the EDPS Privacy by Design is particularly an element of accountability and should be technologically neutral; it should not intend to regulate technology, i.e. it should not prescribe specific technical solutions. On the contrary existing privacy and data protection principles should be integrated into ICT systems and solutions. PbD requirements should apply across sectors, products and services. PbD includes technical and organizational measures, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to ensure the protection of personal data and prevent any unauthorized processing.

Last but not least, the European Commission adopted an Implementing Decision on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management.[18] The mandate points out that the standards should cover privacy issues in different

[17] Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"; Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy.

[18] See M/530 COMMISSION IMPLEMENTING DECISION C(2015) 102 final of 20.1.2015, at http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548#.

phases, including:

– **Definition of product specifications**: identification and definition of privacy requirements and constraints, according to the specific product expected exploitations and the type of data documentation of the privacy specifications;

– **Design of product and components**: allocation of the privacy requirements and constraints to individual components; documentation of the allocation;

– **Development and production of components**: verification and documentation that the allocated privacy requirements and constraints have been implemented accordingly;

– **System integration**: verification and documentation that through the integration of the individual components into the final product/system, and more over through the potential integration of further, external components (e.g. commercials off the shelf (COTS)) including ICT and software the originally specified privacy requirements and constraints are still fully implemented and respected.

– **Testing**: an important phase of product/service development lifecycle may often involve processing personal data and interconnected risks.

The proposed scheme, for each step of the product lifecycle, should identify the relevant data protection risks and propose solutions for their mitigation or, possibly, measures to void the identified risks, something which is part of the PIA exercise that data controllers are called to perform.

c. What is a PIA

A PIA always refers to a process for identifying and evaluating privacy risks, checking privacy legislation and finding solutions to avoid or mitigate these risks. In this project, together with the one contained in Article 35 of the GDPR, we take into account the definition of Wright & De Hert (2012)[19] stating that:

"*A privacy impact assessment is a methodology for assessing the impacts on privacy of project, policy, program, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative impacts*" (Wright & De Hert, 2012).

[19] Wright, D. & De Hert, P. eds., 2012. *Privacy Impact Assessment*, Dordrecht: Springer Netherlands. Available at: http://link.springer.com/10.1007/978-94-007-2543-0.

Several core characteristics of conducting a PIA may be described by the following (PIAF, 2012)[20]:

PIA as a Privacy by Design safeguard

PIA has to be intended as a step "*to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects*", as enshrined by Article 25 of the GPDR on Privacy by design and by default.

PIA is therefore a crucial moment to understand data protection implications of the processes, single out risks and identify remedies.

A PIA should be an on-going process

A PIA should be carried out as a process, and not as a single task of completion. It should start early and continue throughout the development processes.

Scalability

A PIA should be tailored to the organization or project processes. Every organization and project is different, and has different experience in dealing with privacy. The scale and scope of the PIA should thus be appropriate to these circumstances.

Accountability

The ability to demonstrate that a PIA has been carried out adequately by adopting and implementing the appropriate measures and demonstrating that these measures have been implemented

Transparency

A minimum level of transparency should be implemented by, for example, involving stakeholders, publishing the results, etc.

The PIA is now a mandatory process that data controllers have to go through, in certain cases provided for by Article 35 of the GDPR. For more details on the PIA, with a focus on Smart Cities, see infra paragraph 3.

[20] PIAF project, "*Recommendations for a privacy impact assessment framework for the European Union*", Brussels - London, November 2012. Available, at www.piafproject.eu/ref/PIAF_D3_final.pdf.

2 PRIVACY BY DESIGN GUIDELINES FOR SMART CITIES

When running a project and/or initiative which relies or however has an impact on personal data protection, Smart Cities should bear in mind and apply some basic principles.

Key GDPR Principles

1. The GDPR applies to the **processing of personal data wholly or partly by automated means** and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
2. The GDPR have an **extra-territorial reach**, meaning that its rules apply not only to controllers or processors established in the European Union, but also to entities having their establishment in a third country, if they:
    a. Offer goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union (e.g. a US-based social network); or
    b. Monitor the data subjects' behavior, as far as their behavior takes place within the Union (e.g. email tracking service providers)
3. **Personal data cannot be processed without a legal ground**. This usually entails that the data subject has to give his/her **consent** to the processing of his or her personal data for one or more specific purposes; however, different legal grounds may apply, in different instances, which could exempt controllers or processors from collecting the data subject's consent. This holds true when personal data processing:
    a. is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (e.g. when transferring connected cars' data to an external provider of maintenance services, as agreed with the car's owner through a contract);
    b. is necessary for **compliance with a legal obligation** to which the controller is subject (e.g. a Union, national or regional law setting out rules and obligations for cities within smart cities' programs);
    c. is **necessary in order to protect the vital interests of the data subject or of another natural person** (e.g. when deploying IoT devices for emergency health care purposes);

d. processing is necessary for the performance of a **task carried out in the public interest** or **in the exercise of official authority** vested in the controller (e.g. when personal data processing is necessary to manage a tax system);
e. processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (the discipline of the legitimate interest still vary across EU Member States and needs a case by case assessment).

4. **Consent should be free, unambiguous, informed, prior and demonstrable by the data controller**, meaning that it must be documented somehow (also electronically, e.g. by means of a log).
5. In any event, **data subjects must be informed** about the processing undergone by their personal data before the processing starts or, when data are not collected from the data subjects themselves, within a reasonable period, in any event no later than the first communication or the first disclosure to the public, when such activities are foreseen (e.g. in a smart city context, by complete information notices published on the cities' websites, by icons displayed on the users' devices, by signs on the street in correspondence of IoT sensors or cameras).
6. **Data protection principles** (*ie* data minimization, purpose limitation, data accuracy, storage limitation etc.) **must always be respected**; a data controller may have a legal ground to process personal data (e.g. the data subject's consent), yet it may still run the processing in breach of one of the key data protection principles, which would make the personal data processing unlawful and, potentially, trigger a sanction by competent authorities. This is the essence of the principle of **accountability**.
7. The principle of **data protection-by-design is now set in law.** It requires the controller to implement "*technical and organizational measures appropriate to the processing activity being carried out and its objectives, such as data minimization and pseudonymisation, in such a way that the processing will meet the requirements of* [the] *Regulation and protect the rights of (…) data subjects*";
8. Same goes for the principle of **data protection-by-default**, that refers to the amount of data collected, retention period, extent of the processing, data accessibility etc. Essentially,

"*the controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are necessary for each specific purpose of the processing are processed*".

9. Clear procedures must be in place to **ensure data subjects' rights**, namely:
    a. Right of access;
    b. Right to rectification;
    c. Right to erasure;
    d. Right to restriction;
    e. Right to data portability
    f. Right to object
10. Procedures to handle and notify **Data Breaches** to Data Protection Authorities and Data Subjects concerned must be in place.
11. Stakeholders must delete **raw data** as soon as they have extracted the data required for their data processing.

Key ePrivacy Directive principles

1. Where the ePrivacy Directive provides for a specific rule applicable to natural and legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks, it prevails over the general rule set out by the GDPR ("*Lex Specialis derogat generali*"- **Principle of Specialty**);
2. Electronic Communication Services and Networks must be secured through appropriate technical and organizational measures **(Security**);
3. The confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, must be ensured **(Confidentiality);**
4. Access to, or storage of, information into the users' devices must be authorized by the users with a specific consent, unless it is "*strictly necessary in order to provide a service explicitly requested by the subscriber or user*" (also known as "cookie law", **Prior Consent**);
5. **Principles applicable to Traffic Data**

a. Traffic data **must be erased or made anonymous** when it is no longer needed for the purpose of the transmission of a communication or for the purposes of processing subscriber's billing and interconnection payments (**Traffic data erasure**);
b. Traffic data can be processed for marketing and/or for the provision of value added services **only upon specific consent** of the user concerned (**Consent for Marketing purposes**);
c. **Specific information on traffic data processing and its duration** must be provided (**Specific Information**);
d. **Traffic data must be processed only by persons under the authority of the service provider that are dedicated to the function or unit for which such data are necessary** (e.g. handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service – **Authorization profiles**);

6. Principles applicable to **Location Data**:
    a. Location data can be processed for the provision of value added services **only anonymously or upon specific consent** of the user concerned (**Consent for Location Data**);
    b. Users must be given the opportunity to easily refuse such processing at each connection (**Updated Consent**);
    c. Location data must be processed only by persons under the authority of the service provider that are dedicated to the function or unit for which such data are necessary (**Authorization profiles**);

On the specific role of the DPO

Synchronicity has appointed Mandat International as Personal Data Protection Office ("PDPO") of the project. For the purpose of this document we assume that PDPO is the equivalent of DPO. In complex cases, like a smart city, where there are multiple stakeholders with different tasks, responsibilities and abilities to impact on personal data, the appointment of the project's DPO is a necessary but not sufficient condition to have a sound data protection policy and architecture.

On the basis of Article 37 (1) (a) of the GDPR, **cities have the obligation to appoint a DPO,** in that they are public authorities in the reading of that provision.

The other stakeholders should assess whether they have a similar obligation, because:

- they act as public authorities or bodies governed by public law (e.g. a public limited company set up by the city and entrusted with tasks in the field of waste collection and road cleaning; State Research Institutes and/or Universities etc.);
- their **core activities** consist of processing operations which, by virtue of their **nature**, their **scope** and/or their **purposes**, require **regular and systematic monitoring** of data subjects on a **large scale** (Art. 37 (1) (b) of the GDPR);
- their **core activities** consist of processing on a **large scale** of **special categories of data** (*e.g.* health data, genetic data, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership etc) or personal **data relating to criminal convictions and offences** (Art. 37 (1) (c) of the GDPR).

In any event, controllers and processors shall document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly.

More precisely, the project will establish a **network of DPOs** which will include, at least:

a. The Project's DPO;
b. The Cities' DPOs;

And, where possible,

c. The Consortium Members' DPOs, where available and/or required by law;
d. The DPOs of any other stakeholder involved in the smart city initiative, where available and/or required by law.

The network will be coordinated by the project's DPO; the other DPOs will bear the primary responsibility to carry out the activities that the applicable data protection law provides for the appointing entities (i.e. the cities, the consortium's members, the other stakeholders etc).

It is therefore paramount to understand, for each of the entities mentioned above, if they are under the obligation to have a DPO and, if yes, what its role, tasks and position should be, on the basis of

Articles 37 to 39 of the GDPR. [21]

- The relevant stakeholders shall appoint a DPO, on the basis of:
  - **Expert knowledge of national and European data protection laws and practices and an in-depth understanding of the GDPR**;
  - **sufficient understanding of the processing operations** carried out, as well as the information systems, and data security and data protection needs of the controller;
  - **ability to fulfil the tasks** entrusted to him/her by data protection law.[22]
- The data protection officer may be **a staff member** of the controller or processor, or fulfil the tasks on the basis of a **service contract,** on condition that he/she fulfils the requirements and conditions provided for by the law, in particular for what regards the **avoidance of conflicts of interest** and the **expert knowledge of data protection law**. An external consultant enjoys the same status of the staff member and cannot be unfairly dismissed, because of the performance of his/her tasks. [23]
- The DPO contact details shall be **published** by the controller and/or processor and **communicated to the national Data Protection Authority**.[24]

The DPO shall:

- **inform and advise the controller or the processor** and the employees who carry out processing of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions;
- **monitor compliance** with the GDPR and with other Union or Member State data protection provisions
- provide advice where requested as regards the **data protection impact assessment;**
- **cooperate with the supervisory authority and act as its contact point;**

[21] See also Article 29 Working Party, Guidelines on Data Protection Officers ("DPOs"), adopted on 13 December 2016. Available at http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.
[22] See Article 37 (5) of the GDPR.
[23] See Article 37 (6) of the GDPR
[24] See Article 37 (7) of the GDPR

- directly **report** to the **highest management level** of the relevant stakeholder and **not be instructed** by the controller or processor regarding the exercise of his/her tasks.

The DPO shall be provided with all **the necessary resources,** including **financial** ones, to fulfil his/her task independently, to access processed personal data and to maintain his/her specialistic knowledge.

The DPO **shall not be dismissed or penalized** by the controller or the processor **for performing his/her tasks**.

Data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation**.**

The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

The DPO may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties **do not result in a conflict of interests.**[25]

3 PIA METHODOLOGY FOR SMART CITIES

In order to perform a PIA some preliminary issues should be tackled.

The first of such issues is to understand and describe the Target of Evaluation of the PIA, as per paragraph 3.a.

This activity should be carried out by the City's DPO in cooperation with the DPOs of the other involved stakeholders, as per paragraph 3.b below. They should, together, define the objects, services or processes which may need to be assessed.

Once this mapping and description is done, and a clearer knowledge of the data protection critical items is achieved, it is possible to take a decision on whether a PIA is actually due, following the criteria better detailed in paragraph 4 below.

If yes, the PIA framework described in paragraph 5 can be used, and the results thereof reported as per paragraph 7.

[25] See Articles 38 and 39 of the GDPR.

a. Target of Evaluation

The Target of Evaluation is the concrete object of an evaluation from a data protection standpoint. It may be either one or several component(s) of a smart city, like an app, a system of sensors, cameras, an interface, a database etc. The same applies to smart cities' services, such as a service offered to citizens in the context of an efficient traffic management. As the WP29 points out in the *Guidelines on Data Protection Impact Assessment (*hereinafter *"DPIA Guidelines")*, "*a single DPIA could be used to* ***assess multiple processing operations that are similar in terms of the risks presented****, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing*".[26]

For example, a group of municipal authorities setting up a similar network of sensors used to monitor the noise on the streets could carry out a single PIA covering the processing by these separate controllers.

An accurate specification of the target of evaluation is of fundamental importance for the performance of a PIA, as it is the object thereof. At the beginning of the PIA report, the person in charge of the PIA shall accurately determine the ToE and its area of application. It also entails that the data flow resulting from the use of the product or service needs to be illustrated; on that basis, the legal provisions applicable for the processing of personal data will be determined. [27]

The following relevant questions should be answered for each envisaged ToE:

- Does the ToE qualify as an IT product, an IT-based service or processing operation?
  - If the ToE is an IT-based product: Does the product manufacturer qualify as a controller ("controller") or as a processor ("processor") in terms of EU data protection law?
  - If the ToE is an IT-based service: Does the service provider qualify as a controller ("controller") or as a processor ("processor") in terms of EU data protection law?
  - If the ToE is a set of processing operations: do these operations present similar risks? Can they be covered by the same PIA?
- What precisely is the Target of Evaluation?

[26] 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*", p.6.
[27] See also the methodology developed by EuroPriSe in its "*Criteria for the certification of IT products and IT-based services*", https://www.european-privacy-seal.eu/EPS-en/Home.

- What types of personal data are processed when the product or service is used, or when the processing operations take place? Which groups of data subjects are concerned when the product or service is used (e.g., consumers, citizens, travelers, drivers, employees of the service provider)?
- What data flows occur when the product or service is used?

b. Stakeholders in a Smart City scenario

This section takes stock of the discussion held within Task 1.2. of Synchronicity, which led to the adoption of the Synchronicity Architecture.

Together with the partners active on the mentioned task, the following stakeholders have been identified in a smart city scenario:

- **Cities.** Cities are the primary entities within a smart city initiative, in that they set the general purposes and means of the latter, have the big picture of all the involved stakeholders and can start or discontinue the relevant smart city project. From a data protection viewpoint they shall be considered as the data controllers in so far they process personal data in the context of the project. Yet even when they do not practically process personal data, their role is data protection critical because they are in the position to determine purposes and means which are later on pursued by the other stakeholders.
- **Citizens.** From a data protection perspective, they are data subjects and or users. This category may be further split in two, in order to distinguish between:
    - Active Citizens, meaning those actively participating to the smart city initiative;
    - Inactive citizens, meaning those whose personal data are accidentally or systematically collected by sensors or other data captors without their active engagement.
- **Urban utilities:** Companies providing public services in the cities are key players in making the cities more efficient and sustainable. Either outsourced (public procurement) or just public (belonging to the municipalities) they tend to integrate IoT technology for improving service performance. As such, they become natural data generators (collecting data), data consumers (interacting with other public services in the cities aiming at improving the whole ecosystem) and data providers to third parties. Last but not least, they are also technology consumers**.**

- **LPWAN operators and service providers**: Operators and service providers play a central role in either generating, collecting and providing data linked to the information interchange (operators) and service provision.
- **Universities:** Academic institutions are often associated to smart cities' projects with various roles, e.g.as scientific coordinators, testbeds managers, etc.
- **App developers.** Users of smart cities services often have to install third-party applications which enable them to access their data, as stored by the device manufacturer. Installing these applications often consists in providing the app developer with an access to the data through the API**.**
- **Marketing research & customer segmentation companies.** The great amount of information generated in the context of a smart city may turn very useful for stakeholders specialized in customers' behavioral analysis and segmentation. This can lead to the setting up of databases containing profiled information on data subjects which, in turn, are very useful to derive business intelligence insights. Such information may be collected through smart cities' deployments and processed in an anonymous fashion (e.g. as aggregated data) or in clear mode; in the latter case, personal data protection issues arise and need to be tackled

With the exclusion of the citizens, from a data protection viewpoint all the stakeholders listed above may bear the role of data controllers or data processors, depending on what they do with personal data, and with what is their degree of autonomy and control over personal data processing.

4 PRELIMINARY ISSUES

a. Is a PIA legally necessary?

According to Article 35 (1) of the GDPR, "*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is **likely to result in a high risk to the rights and freedoms of natural persons**, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. **A single assessment may address a set of***

similar processing operations that present similar high risks".

Further in the Article (paragraph 3, letter c) it can be read that "*a data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of (…)* ***a systematic monitoring of a publicly accessible area on a large scale****".*

This may well be the case of a smart city initiative.

> Therefore, in order to understand if a PIA is due, it is first of all necessary to assess whether the Smart City initiative at stake entails a systematic monitoring of a publicly accessible area on a large scale by means of sensors, cameras and other objects; it can be reasonably assumed that **for Smart Cities a PIA is necessary.**

The following diagram explains the PIA process.

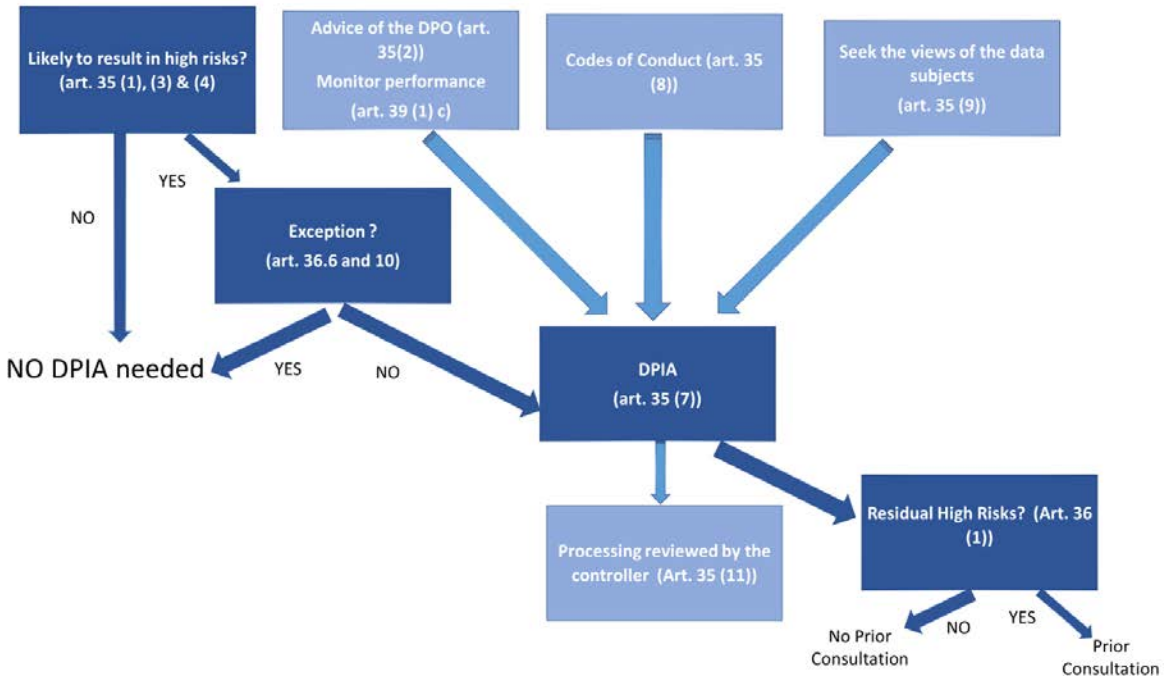

Figure 1 - PIA Diagram, WP29, DPIA Guidelines

Further to the criterion of a ***systematic monitoring of a publicly accessible area on a large scale*** explained above, in appraising whether a PIA is necessary the following additional criteria should be considered, as indicated by the WP29. [28]

1. Evaluation or scoring, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements" (recitals 71 and 91 GDPR). Examples of this could include a bank that screens its customers against a credit reference database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.

2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person" (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion.

3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through "a systematic monitoring of a publicly accessible area" (Article 35(3)(c))13. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in frequent public (or publicly accessible) space(s).

4. Sensitive data: this includes special categories of data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. This criterion also includes data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data, financial data (that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly

[28] WP29, DPIA Guidelines, pp.7-9.

available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include information processed by a natural person in the course of purely personal or household activity (such as cloud computing services for personal document management, email services, diaries, e-readers equipped with note-taking features, and various life-logging applications that may contain very personal information), whose disclosure or processing for any other purpose than household activities can be perceived as very intrusive.

5. Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

i. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;

ii. the volume of data and/or the range of different data items being processed;

iii. the duration, or permanence, of the data processing activity;

iv. the geographical extent of the processing activity.

6. Datasets that have been matched or combined, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.

7. Data concerning vulnerable data subjects (recital 75 GDPR): the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data. For example, employees would often meet serious difficulties to oppose to the processing performed by their employer, when it is linked to human resources management. Similarly, children can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data. This also concerns more vulnerable segment of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly, a patient, or in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.

8. Innovative use or applying technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.

9. Data transfer across borders outside the European Union (recital 116), taking into consideration, amongst others, the envisaged country or countries of destination, the possibility of further transfers or the likelihood of transfers based on derogations for specific situations set forth by the GDPR.

10. When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and recital 91 GDPR). This includes processings performed in a public area that people passing by cannot avoid, or processings that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

The WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA. As a rule of thumb, **a processing operation meeting less than two criteria may not require a DPIA** due to the lower level of risk, and processing operations which meet at least two of these criteria will require a DPIA

b. Possible Exceptions to the PIA obligation

Article 35 provides for some exceptions to the PIA.

The first exception is set forth by Article 35 (5), whereby it Is stated that "*The supervisory authority may also establish and make public a list of the kind of processing operations for which no data*

protection impact assessment is required. The supervisory authority shall communicate those lists to the Board".

It shall be therefore checked whether the personal data processing (or sets of processing) entailed by the Smart City are covered by one of these lists, once they are drawn up and published. So far, the DPAs of the European Member States have not exercised this prerogative yet.

The second exception is likely more relevant for Smart Cities; it stems from Article 35 (10) GDPR which lifts data controllers from the obligation to carry out a PIA when "*the processing has a **legal basis in Union law or in the law of the Member State to which the controller is subject**, and that law regulates the specific processing operation or set of operations in question, and **a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis***".

Smart Cities' are very often the result and/or the objective of public policies which may have their foundations in formal acts of legal nature adopted by local, national or European public authorities.

When this is the case, the following two conditions must be met in order for the exception to the PIA to apply:

- ✓ The legal basis for a certain smart city initiative must be provided for by Union or Member State law;
- ✓ The law has been adopted after a data protection impact assessment, as part of a general impact assessment.

This triggers two questions.

- ✓ **What kind of acts can be considered Union or Member State law?**

The notion of law must be interpreted widely; it encompasses written and unwritten legal rules which are applicable in a given system (Union or Member State) according to its own constitutional criteria on the production and hierarchy of norms.

As a result, not only legislative acts adopted pursuant the ordinary or special legislative procedures provided for by the Treaty on the Functioning of the EU ("TFEU") are to be considered Union law, but also secondary acts, such as European Commission's delegated or implementing acts can amount to Union law in the reading of Article 35 GDPR.

Similarly, Member State law not only encompasses legislative acts adopted at national level, but also secondary laws or administrative rules, such as regulations, circulars, city councils' resolutions, as well as regional laws, depending on the definition of law provided for by the domestic legal order. Another factor to be considered is that, pursuant to Recital 45 of the GPDR, "*the Regulation does not require a specific law for each individual processing*", and therefore one law may contain the legal basis for several data processing.

> It shall be verified whether the personal data processing takes place on the basis of a law adopted by the competent Union or Member State authority; the concept of law should be widely interpreted, so as to encompass any enforceable source of rules adopted pursuant to the constitutional framework of the legal system under consideration (i.e. the EU Treaties, legislative and non legislative acts for Union law, national constitutions, ordinary and secondary laws for Member States' law).

- ✓ **What is a general impact assessment? And when a data protection impact assessment can be deemed performed in the adoption of a legal basis?**

An example of what is a general impact assessment for envisaged legislation can be found in the procedure usually followed by the European Commission when appraising the policy options before presenting a legislative proposal. In its Impact Assessments, the European Commission usually identifies the objectives of the envisaged reform, the issues to be tackled to improve the existing regulatory framework and the best policy approach to be undertaken, in the light of the issues to be solved and of the objectives to be achieved.[29]

So far, the European Commission has not carried out any data protection impact assessment as a part of the general ones.

A data protection impact assessment may be particularly relevant for those legal instruments that set up systems, databases, complex initiatives or procedures which rely on personal data processing. An example thereof is the Commission's Proposal[30] to revise the EURODAC system

[29] See, for example, the "Impact assessment on the reform of the data protection regulatory framework" http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.

[30] See the Proposal for a Regulation of the European Parliament and of the Council on amending Regulation (EU) No 603/2013 on the establishment of Eurodac for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013] establishing the criteria and mechanisms for determining the

database[31] which, according to the European Data Protection Supervisor ("EDPS") should require a prior data protection impact assessment. [32]

From a general reading of the GDPR it can be inferred that such an assessment, performed at the early stage of the legislative process, is functional to the adoption of rules that embed those data protection elements and safeguards foreseen by Recital 45 of the GDPR, whereby it is set out that *"(…) A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient.* ***It should also be for Union or Member State law to determine the purpose of processing****. Furthermore,* ***that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law****, or,* ***where it is in the public interest to do so****, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association*".

This recital is a short manual of *privacy-by-designed* law making, which presupposes a DPIA beforehand.

In conclusion, it must be ascertained if, in the adoption of Union or Member State law, the competent rule maker has carried out a data protection impact assessment of that legal basis, also as part of a general impact assessment of the same kind of the ones usually performed by the European Commission.

Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person, for identifying an illegally staying third country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast 2016) ('the Eurodac Recast 2016 Proposal').

[31] Eurodac is the EU asylum fingerprint database, established by Regulation (EU) No 603/2013. It is currently under revision.

[32] See EDPS, Opinion of the European Data Protection Supervisor on the first reform package on the Common European Asylum System(Eurodac, EASO and Dublin regulations), issued on 12.1.2017, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017XX0112(01)&from=EN.

However, even when such assessment is performed while making the law, it is likely to require a review before the entry into operations, as the adopted legal basis may differ from the proposal in ways that affect the impact on privacy and data protection (WP29, DPIA Guidelines).

c. On the expertise of the person(s) in charge of the PIA

Carrying out a PIA requires the interaction of different stakeholders and competences. For example, assessing a large scale database, where the information collected within the city flows, require the intervention of multiple expertises, such as, by way of example:

- the project coordinator(s), *ie* the person(s) in charge of managing the entire project, who has/have the big picture of it;
- the different legal/compliance officers within the entities associated to the project, such as the waste management company, the hosting provider company, the telecommunication services' provider company, the company managing parking spots etc;
- the Data Protection Officers within the entities associated to the project, where available;
- the different IT officers within the entities associated to the project;
- staff with a responsibility for risk management within the entities associated to the project;
- the designers of the project / system within the entities associated to the project;
- procurement staff within the entities associated to the project;
- staff with a responsibility for communications within the entities associated to the project;
- senior management of the entities associated to the project.

In order to ensure uniformity to the PIA process, all the involved stakeholders should be coordinated at a double level by:

- the **Smart City's DPO**, who should lead the process and coordinate all the stakeholders;
- the **DPOs of each of the entities** associated to the project, where appointed.

If a DPO is not appointed within the entities associated to the project, the process should in any event be chaired, for each stakeholder, by a person who has expert knowledge of data protection law and practices and is able to provide guidance on data protection related matters, as well as to monitor the application of the data protection legal framework to the project.

d. Why it is anyway recommended to perform a PIA

There exists a number of important benefits when performing a PIA, namely:

- Preventing costly adjustments in processes or system redesign by mitigating privacy and data protection risks
- Prevention of discontinuation of a project by early understanding the major risks.
- Reducing the impact of law enforcement and oversight involvement
- Improving the quality of personal data (minimization, accuracy)
- Improving service and operation processes
- Improving decision - making regarding data protection
- Raising privacy awareness within the organization
- Improving the feasibility of a project
- Strengthening confidence of consumers, employees or citizens in the way which personal data are processed and privacy is respected
- Improving communication about privacy and the protection of personal data.

This approach is endorsed by the WP29, which states that "*In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers comply with data protection law*".[33]

5 PIA FRAMEWORK FOR SMART CITIES

Each of the ToE, as identified according to paragraph 3 (a), need to be assessed by the relevant persons as per paragraph 3 (c) above, against the checklist and methodology defined in the following paragraphs a, b, c, d and e.

A. Description of the envisaged processing operations and the purposes of the processing

A full understanding of how information will be used is needed. An answer should be given to the following questions:

i. Has the **purpose** of the project / process been identified? What is it intending to achieve?
ii. How will information be **collected**, **used** and **retained**? It is important to identify all of the purposes for which the information might be used in the future.

[33] WP29, DPIA Guidelines, p.7.

iii. If the processing involves **marketing**,[34] is there a procedure for individuals to opt out of their information being used for that purpose?

iv. How will the **accuracy** of the personal data to be obtained from individuals or other organizations be ensured?

v. If **communication** of data will be made to other people or stakeholders, how will the data be adequately **protected**?

vi. Will the project require data to be transferred **outside of the European Union**? (This includes potentially placing data on the **internet** or in the **cloud**) If so, under what safeguards will the transfer be made?

vii. **How many** individuals will be affected?[35]

viii. How will individuals be **informed** about the use of their personal data?

ix. What are those individuals' **reasonable expectations** with regards to the data?[36]

x. What are the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels)?

xi. Do any of the stakeholders involved in the processing adhere to a data protection code of conduct?

B. Legal grounds of processing

The legal basis of the personal data processing carried out within, through or in the context of the ToE must be described.

b.1 Processing on the Basis of Consent (Article 6(1)(a) and 7 GDPR)

i. Is the data subject asked to give consent to the processing of his or her personal data for one or more specific purposes?

ii. If so: Does the consent as expressed by the data subject meet the legal requirements for consent?

1. Is the consent freely given? [37]

[34] It may occur, for example, when the habits of users of public transport services are tracked and profiled by means of the information provided by the ticketing system, and thereafter used to perform behavioral advertising.

[35] This figure may be expressed in absolute numbers, or as a proportion of the relevant population.

[36] To answer to this question, the results of the open consultation referred to in paragraph 6 can be taken into account.

2. Does the data subject have a genuine or free choice or is the consent obtained under some form of duress or threat of disadvantage?
3. Is there a clear imbalance between the data subject and the service provider, in particular where the provider is a public authority? Is it therefore unlikely that consent was/is freely given in all the circumstances of the specific situation?
4. Provided that this is appropriate in the individual case, does the data subject have the possibility to give separate consent to different personal data processing operations?
5. Is the performance of a contract, including the provision of a service, conditional on consent to the processing of personal data that is not necessary for the performance of that contract?
6. Is the data subject able to refuse or withdraw consent without detriment?
7. Is the consent sufficiently specific, by setting out the purpose(s) of the various phases of the processing?
8. Is the consent informed?
9. Is the data subject made aware of all relevant aspects of the data processing for which the personal data are intended and at least of the identity of the service provider and the purposes of the processing?
10. If the data subject's consent is given in the context of a written declaration which also concerns other matters: Is the request for consent presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, and using clear and plain language?
11. Are safeguards in place, particularly in the context of a written declaration on another matter, that ensure that the data subject is aware of the fact that and the extent to which consent is given?

[37] For example, if the controller makes the provision of a service dependent on the data subject's consent for marketing activities, that consent is not freely given. See also question ii.5 below.

12. If a declaration of consent is pre-formulated by the service provider[38] in the context of a consumer contract, is it provided in an intelligible and easily accessible form, using clear and plain language and does the service provider refrain from the use of unfair terms?
13. Is the data subject informed of his or her right to withdraw consent at any time prior to giving consent? In addition, is the data subject informed that withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal?
14. Is the consent unambiguously given? Does the data subject signify agreement to the processing of personal data relating to him or her by a statement or by a clear affirmative action?[39]
15. Is the controller able to demonstrate that the data subject has consented to the processing of his or her personal data?

b.2 Processing on the Basis of a Contract (Article 6(1)(b) GDPR)

i. Is the processing of personal data necessary for the performance of a contract to which the data subject is party?
ii. Is the processing of personal data necessary in order to take steps at the request of the data subject prior to entering into a contract?
iii. Is the processing of each type of personal data involved necessary for the above-mentioned purposes?

b.3 Processing on the Basis of Legal Obligation (Article 6(1)(c) GDPR)

i. Is the processing of personal data necessary for compliance with a legal obligation to which the service provider is subject?
    1. What legal provision does establish the obligation? Does it have a basis in Union or Member State law? Does Union or Member State law determine the purpose of the processing? [40]

[38] In the context of this PIA framework, the service provider may either be a data controller or a data processor, and also referenced as such in the questions.
[39] For example, bypassing an informative banner, or by checking-in through the electronic travel card etc.
[40] In replying to this question it will turn useful the preliminary analysis carried out as per paragraph 4.a.

2. Does the law establish specifications for determining the type(s) of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing?
3. If so, does the service provider ensure compliance with these specifications (e.g. by not providing for “free fields”)?
4. If the law does not itself specify what data may be collected: Is the processing/are the data really necessary to meet the obligation?

ii. Does/may the intended use of the product or service require/involve the processing of personal data that is necessary for compliance with a legal obligation which has a basis in Union or Member State law and to which the user of the product or service is/may be subject?

b.4 Processing on the Basis of Vital Interests (Article 6(1)(d) GDPR)

i. Is the processing of personal data necessary in order to protect the vital interests of the data subject or of another natural person?

ii. What are the relevant vital interests?

iii. Is it necessary to rely on this criterion, or can the consent of the data subject be obtained?

iv. If the processing is based on the vital interest of another natural person: Is it necessary to rely on this criterion, or can the processing be manifestly based on another legal ground?

b.5 Processing on the Basis of a Public Task (Articles 6(1)(e), (2)+(3) and 36(5) GDPR)

i. Is the processing of personal data necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller?

ii. Is the basis for the processing laid down by Union law or Member State law to which the controller is subject? What is the relevant legal provision?

iii. Does the law establish specifications for determining the type(s) of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitation, the storage period and processing

operations and processing procedures, including measures to ensure lawful and fair processing?

a. If so, does the service provider ensure compliance with these specifications (e.g. by not providing for “free fields”)?

b. If the law does not establish said specifications: Is the processing / are the data really necessary for the performance of that public task?

iv. Does Member State law require the service provider to consult with, and obtain prior authorization from, the supervisory authority?

a. If so, has the service provider consulted with and obtained prior authorization from the competent supervisory authority?

b.6 Processing on the Basis of Balancing of Interests (Article 6(1)(f) GDPR)

This legal ground is **not applicable** to a service provider that is a **public authority** and carries out the processing in the performance of its tasks. If the service provider **is not** a public authority, please reply to the questions below.

i. Is the processing of personal data necessary for the purpose(s) of the legitimate interests pursued by the service provider or by a third party? More precisely:

a. What legitimate interests of the service provider or of a third party are served by the processing?

b. What fundamental rights and interests of the data subjects are affected by the processing?

c. Is the right balance struck between these competing interests (i.e. are the legitimate interests of the service provider not overridden by the rights and interests of the data subjects)?

C. Necessity and proportionality assessment

This assessment entails a legal evaluation of the intended personal data processing that shall be carried out by the by the relevant persons as per para 3 (c) above. In particular, such assessment

should take into account the guidance provided for by European Union case law[41] on the principle of necessity and proportionality in data protection law.

When carrying out this legal assessment, the following criteria/elements should be taken into account. The list of questions should be deemed as a supporting tool. It can be enriched by further legal considerations of the evaluator and each question requires extensive explanation by the latter:

i. Is the intended personal data processing **necessary** to achieve the objectives pursued by the data controller? More precisely:
    a. Is/was the objective pursuable by means of processing of non-personal data? Is there a least intrusive means to achieve the same objective?
    b. Is the amount of personal data collected limited to what is necessary?
    c. Is the objective provided for by law in the pursuit of a public interest? What is the public interest at stake and why it makes it necessary to process personal data?
    d. Is the data storage duration limited?

In replying to the questions above, it should be considered that:

- Not everything that "might prove to be useful" for a certain purpose is "necessary". Mere convenience or cost effectiveness is not sufficient.
- The selected categories of persons affected, the categories of personal data collected and processed, the storage period of the data, etc., should effectively contribute to achieve the aim pursued.
- If the proposed measure includes the processing of sensitive data, a higher threshold should be applied in the assessment of effectiveness.
    - Sensitive data encompass amongst others data revealing: ethnic or racial origin, political opinions, religious or similar beliefs, health status. Data relating to criminal convictions and offences have a similar status. Genetic and biometric data are recognised as sensitive data by the GDPR.
    - Other categories of data, although not strictly categorised as sensitive, in certain contexts may present a higher risk for the individual and trigger the application of a

[41] See, amongst the many, *Joined Cases C-293/12 and C-594/12 "Digital Rights Ireland"; Joined Cases C-92/09 and C-93/09, "Schecke*."

higher threshold of what is strictly necessary. This is the case, for instance, of unique identifiers.[42]

ii. Is the intended personal data processing **proportionate** in pursuing the objectives of the data controller? More precisely:

a. Is access to personal data limited only to authorized persons?

b. Are technical safeguards applied to personal data, such as pseudonymisation?

c. If personal data are transferred outside the European Union, under what safeguards the transfer is performed?[43]

d. How are data subjects' rights respected (i.e. right of access and portability, right to rectify, erase, object, restriction of processing)?

D. Assessment of the risks to the rights and freedoms of data subjects

The risk analysis is an important part of the PIA. It allows to identify threats to privacy and personal data protection. A good risk analysis requires a precise and sound description of the envisaged processing, and relies on the expertise and independence of the PIA assessor. The risk analysis should assess both the impact on individuals and on the society as a whole, especially in the context of Smart Cities.

Please describe if the data subjects or the society run one or more of the following risks and how they could be affected.

Description of risk	Likelihood/impact of risk (Low/Medium/High)	Severity of the risk (Low/Medium/High)
Accidental or unlawful destruction of personal data		
Loss of personal data		
Alteration of personal data		

[42] See also EDPS, "*Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*", issued on 11 April 2017, p.17.
[43] See also question vi in paragraph 5.A.

Unauthorized disclosure of, or access to, personal data		
Financial loss		
Discrimination		
Identity Theft		
Damage to the reputation		
Breach of professional secrecy		
Unauthorised reversal of pseudonymisation		
Other risks (please describe)		

If these risks should materialize, may they lead to physical, material or non-material damage? *Please describe*.

E. Measures envisaged to address the risks

After the risk assessment is carried out, the following step is to identify controls, options and alternatives that can help to minimize, mitigate or eliminate the identified privacy and data protection risks (referred to as "Countermeasures" below). Countermeasures are either of a technical or non technical nature. "*Technical controls are incorporated into the project, e.g. access control mechanisms, authentication mechanisms and encryption methods. Non technical controls, on the other hand, are management and operational controls, e.g. policies or operational procedures. Controls can be categorized as being preventive or detective. The former inhibit violation attempts, while the latter warn operators about violations or attempted violations*". [44]

Please describe, for each of the identified risks, what measures are taken to address them.

[44] PIAF project, "*Recommendations for a privacy impact assessment framework for the European Union*", Brussels - London, November 2012, p.30. Available, at www.piafproject.eu/ref/PIAF_D3_final.pdf.

	Description of risk	Countermeasures
Risk 1	Accidental or unlawful destruction of personal data	
Risk 2	Loss of personal data	
Risk 3	Alteration of personal data	
Risk 4	Unauthorized disclosure of, or access to, personal data	
Risk 5	Financial loss	
Risk 6	Discrimination	
Risk 7	Identity Theft	
Risk 8	Damage to the reputation	
Risk 9	Breach of professional secrecy	
Risk 10	Unauthorised reversal of pseudonymisation	
Risk 11	Other risks (please describe)	

Example of solutions: reduction of data collected; short retention period; destruction of data at regular intervals; security measures; staff training and guidance on the ToE; adherence to a certification mechanism or to a code of conduct; pseudonymisation of data; anonymisation of data; campaigns and measures to increase data subject awareness; easy opt-out for data subjects; agreements / contracts in place with external data controllers or processors, including data sharing agreements; consultation with internal/external stakeholders.

6 POTENTIAL DATA SUBJECTS' PARTICIPATION IN THE PIA, HOW TO INCLUDE THEM?

According to Article 35 (9) of the GDPR "*Where appropriate, the controller shall seek the views*

of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations".

Open Consultation of citizens

One way to involve data subjects and/or their representatives in the PIA process could be for the cities to launch an **open consultation** on the envisaged processing of personal data, before starting it.

The open consultation should take place through the cities' websites, and be organized around the following phases:

Phase 1: Description of the envisaged personal data processing

The cities describe to the general public what objectives they intend to achieve, what personal data they purport to process, and on what legal ground they intend to rely. This description already entails a certain level of data protection impact assessment by the cities, as per Article 35 (7) (a) of the GDPR.

Phase 2: Collect the participants' feedback on the envisaged personal data processing

In this phase it is first of all relevant to ask the participants what role they bear in expressing their views. This will help the cities in mapping the landscape of "engaged" parties within their boundaries, to establish contacts with them, and to weigh the contributions by the level of expertise of the participants.

The participants' feedback should be sought by means of a short list of simple questions which may later on be useful, for those entities who actually carry out a proper PIA, in getting knowledge of potential risks for personal data processing and devising appropriate countermeasures.

The following questions may be raised through an open consultation.

i. Please express your view on the objectives of the envisaged processing. Do you think that the city would provide you with a good service in pursuing them? Would you change anything? If yes, what?
ii. What kind of your personal data are you willing to share with the city and its industrial/commercial partners in the pursuit of the smart city's objectives?
iii. What kind of risks you think you run in using the described smart cities' services?
iv. What would make you feel more comfortable or more protected when using the described smart city's services?

Phase 3: Make a report of the answers collected during the open consultation phase

The Report will be useful to help the cities and the other stakeholders in having a systemic view on the perception of the envisaged initiative.

Phase 4: Take the report's result into account when performing the PIA

The open consultation's outcome is a good input for the professionals that carry out the PIA, because it maps the concerns spread within the public on the envisaged processing. In the PIA the cities and their stakeholders can provide explanations to the wide public on why, for example, a certain risk perceived by the public was considered as not likely by the experts, or what the involved entities plan to do to reduce a risk that they consider likely, together with the public. A similar exercise could serve to increase the democratic participation in designing initiatives that have an impact on people's daily lives and may constitute a good tool to increase awareness on data protection issues within the public.

Meetings or workshops with the data subjects' representatives

A different way to involve the data subjects in the PIA process could be the organization of dedicated meetings, or workshops, with those entities[45] whose statutory objectives are in the public interest and are active in the field of the protection of personal data.

According to the Recital 142 of the GDPR, these entities could, for example, receive a mandate by the data subject to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. When Member State's law provides so, these entities may even exercise the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where they have reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes the GDPR.

These are quite important tasks that the GDPR, or Member State's law, entrust to these entities.

It seems consequential, once these entities become operational under the conditions set by the GDPR or by Member State law, to involve them in the context of a PIA for smart cities, through **dedicated workshops** where the envisaged processing is presented and their feedback collected.

Moreover, when the personal data processing may also impinge on the rights and freedoms of workers (e.g. the cities' staff or the staff of any other stakeholder), the staff representatives or trade/labour unions should be consulted by formal questions or by a survey.

7 REPORTING OF PIA'S RESULTS[46]

a. Results and reporting obligations

[45] Not-for-profit bodies, organisations or associations which are constituted in accordance with the law of a Member State, have statutory objectives which are in the public interest and are active in the field of the protection of personal data.
[46] See also CNIL's Manual on how to carry out a PIA. Available at https://www.cnil.fr/fr/node/15798.

Once identified the risks, and the possible countermeasures to them, the data controller should draw a conclusion and choose amongst one of the following possibilities.

Option 1 - The PIA is deemed acceptable: action plan

Option 2 - The PIA is not deemed acceptable: consult with the Data Protection Authority

b. Formats

Depending on the PIA's outcome, one of the two following formats can be used.

Option 1 - The PIA is deemed acceptable: action plan

Countermeasure	Controller[47]	Difficulty	Financial Cost	Term	Progress

The scales below can be used to develop the action plan and monitor its implementation:

Criteria	Level 1	Level 2	Level 3
Difficulty	Low	Moderate	High
Financial Cost	Nil	Moderate	High
Term	Quarter	Year	3 years
Progress	Not Started	In progress	Completed

The wording below shows a way of carrying out the formal validation of the PIA

Validation of the PIA	On [date], [identity or function] validates the PIA in the light of the study conducted and the PIA report. The processing should allow [synthesis of stakes]. The manner in which it is planned

[47] The controller here is the person/function in charge to apply/monitor the countermeasure.

	to implement the legal requirements and treat the risks is deemed acceptable in view of these stakes. The implementation of the action plan as well as the continuous improvement of the PIA will be demonstrated. [Signature]

Option 2 - The PIA is not deemed acceptable: consult with the Data Protection Authority

Whenever the data controller cannot find sufficient measures (i.e. when the residual risks are still high), consultation with the supervisory authority will be necessary, pursuant to Article 36 GDPR.[48]

Moreover, the controller will have to consult the supervisory authority whenever Member State law requires controllers to consult with, and/or obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health (Article 36(5) GDPR).

It should however be stated that regardless of whether or not consultation with the supervisory is required based on the level of residual risk, then the obligations of retaining a record of the DPIA and updating the DPIA in due course remain.

c. Dissemination

The summary of the PIA's results can be disseminated to the public via the city website or by means of any of the apps connected by the citizens to a certain smart city deployment. As a way to ensure transparency and full information on the smart city's objectives and the safeguards applied to personal data processing, the cities may provide for QR codes in the vicinity of sensors, cameras or other smart city's components, through which the users may access the PIA's Results and the Privacy Policy of the Smart City project at stake.

[48] WP29, DPIA Guidelines, p.18.

8 CONCLUSIONS AND NEXT STEPS

This framework has been drafted by taking into account the best available general PIA frameworks, and further refined with the contribution of the cities' representatives in Synchronicity.

It endeavors to provide the cities with a ready-to-use tool, which can be handled by the cities' DPOs, together with the other DPOs interested by the processing. It can be also used as a support or a refinement of already existing practices within the cities, which remain the entities accountable for the process in the last instance.

Even though the PIA will become a mandatory compliance action only after May 2018, this framework should be nonetheless tested and applied beforehand within Synchronicity, and the results thereof made public on the project's website as well as on the website of each involved stakeholder.

It is furthermore crucial to understand that PIA is a living process, which does not end once the first assessment is made. In fact, the implementation of the countermeasures should be monitored. A PIA should be revisited each time a project is changed and such a change impacts privacy.

ANNEX 1 - PIA FRAMEWORK FOR SMART CITIES

I. Identify the Target of Evaluation ("ToE")

Q.I.1. Does the ToE qualify as an IT product or as an IT-based service or processing operations?

Q.I.1.a. If the ToE is an IT-based product: Does the product manufacturer qualify as a controller ("controller") or as a processor ("processor") in terms of EU data protection law?

Q.I.1.b. If the ToE is an IT-based product: Does the service provider qualify as a controller ("controller") or as a processor ("processor") in terms of EU data protection law?

Q.I.1.c. If the ToE is a set of processing operations: do these operations present similar risks? Can they be covered by the same PIA?

Q.I.2. What precisely is the Target of Evaluation?

Q.I.3. What types of personal data are processed when the product or service is used? Which groups of data subjects are concerned when the product or service is used (e.g., consumers, citizens, travelers, drivers, employees of the service provider)?

Q.I.4. What data flows occur when the product or service is used?

Q.I.5. What is the area of application of the product or service (*e.g.*, is the product or service to be used in the medical or in the advertising sector)?

II. Preliminary Issues

Q.II.1. Is the PIA legally necessary? (see paragraph 4.a. above)

Q.II.1.a. In particular, does the processing entail two or more of the following:

- ✓ Evaluation or scoring, including profiling and predicting
- ✓ Automated-decision making with legal or similar significant effect
- ✓ Systematic monitoring
- ✓ Sensitive data
- ✓ Data processed on a large scale
- ✓ Datasets that have been matched or combined
- ✓ Data concerning vulnerable data subjects
- ✓ Innovative use or applying technological or organisational solutions
- ✓ Data transfer across borders outside the European Union
- ✓ The processing in itself "prevents data subjects from exercising a right or using a service or a contract"

If yes, please proceed to Q.II.1.b. If No, PIA is not obligatory, but still recommended.

Q.II.1.b Does the exception to PIA apply, pursuant to Article 35(10) of the GDPR? (see paragraph 4.b. above)

If yes, PIA is not obligatory, but still recommended. If NO, please proceed to Q.II.2. and then to Q.III.1.

Q.II.2. What is the expertise of the person(s) in charge of the PIA? (see paragraph 4.c. above)

III. PIA Framework for cities

Q.III.1. Description of the envisaged processing operations and the purposes of the processing

Q.III.1.a. Has the **purpose** of the project / process been identified? What is it intending to achieve?

Q.III.1.b. How will information be **collected**, **used** and **retained**? It is important to identify all of the purposes for which the information might be used in the future.

Q.III.1.c. If the processing involves **marketing**,[49] is there a procedure for individuals to opt out of their information being used for that purpose?

Q.III.1.d. How will the **accuracy** of the personal data to be obtained from individuals or other organizations be ensured?

Q.III.1.e. If **communication** of data will be made to other people or stakeholders, how will the data be adequately **protected**?

Q.III.1.f. Will the project require data to be transferred **outside of the European Union**? (This includes potentially placing data on the **internet** or in the **cloud**) If so, under what safeguards will the transfer be made?

Q.III.1.g. How many individuals will be affected?[50]

Q.III.1.h. How will individuals be **informed** about the use of their personal data?

Q.III.1.i. What are those individuals' **reasonable expectations** with regards to the data?[51]

Q.III.1.l. What are the **assets** on which personal data rely (hardware, software, networks, people, paper or paper transmission channels)?

Q.III.1.m. Do any of the stakeholders involved in the processing adhere to a data protection **code of conduct**?

Q.III.2. Legal grounds of processing

Q.III.2.a. Processing on the Basis of Consent (Article 6(1)(a) and 7 GDPR)

Q.III.2.a.i. Is the data subject asked to give consent to the processing of his or her personal data for one or more specific purposes?

Q.III.2.a.ii. If so: Does the consent as expressed by the data subject meet the legal requirements for consent?

Q.III.2.a.ii.a Is the consent freely given? [52]

[49] It may occur, for example, when the habits of users of public transport services are tracked and profiled by means of the information provided by the ticketing system, and thereafter used to perform behavioral advertising.

[50] This figure may be expressed in absolute numbers, or as a proportion of the relevant population.

[51] To answer to this question, the results of the open consultation referred to in paragraph 6 above can be taken into account.

Q.III.2.a.ii.b Does the data subject have a genuine or free choice or is the consent obtained under some form of duress or threat of disadvantage?

Q.III.2.a.ii.c Is there a clear imbalance between the data subject and the service provider, in particular where the provider is a public authority? Is it therefore unlikely that consent was/is freely given in all the circumstances of the specific situation?

Q.III.2.a.ii.d Provided that this is appropriate in the individual case, does the data subject have the possibility to give separate consent to different personal data processing operations?

Q.III.2.a.ii.e. Is the performance of a contract, including the provision of a service, conditional on consent to the processing of personal data that is not necessary for the performance of that contract?

Q.III.2.a.ii.f Is the data subject able to refuse or withdraw consent without detriment?

Q.III.2.a.ii.g Is the consent sufficiently specific, by setting out the purpose(s) of the various phases of the processing?

Q.III.2.a.ii.h Is the consent informed?

Q.III.2.a.ii.i Is the data subject made aware of all relevant aspects of the data processing for which the personal data are intended and at least of the identity of the service provider and the purposes of the processing?

Q.III.2.a.ii.l If the data subject's consent is given in the context of a written declaration which also concerns other matters: Is the request for consent presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, and using clear and plain language?

Q.III.2.a.ii.m Are safeguards in place, particularly in the context of a written declaration on another matter, that ensure that the data subject is aware of the fact that and the extent to which consent is given?

Q.III.2.a.ii.n If a declaration of consent is pre-formulated by the service provider[53] in the context of a consumer contract, is it provided in an intelligible and easily accessible form, using clear and plain language and does the service provider refrain from the use of unfair terms?

---

[52] For example, if the controller makes the provision of a service dependent on the data subject's consent for marketing activities, that consent is not freely given. See also question ii.5 below.

[53] In the context of this PIA framework, the service provider may either be a data controller or a data processor, and also referenced as such in the questions.

Q.III.2.a.ii.o Is the data subject informed of his or her right to withdraw consent at any time prior to giving consent? In addition, is the data subject informed that withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal?

Q.III.2.a.ii.p Is the consent unambiguously given? Does the data subject signify agreement to the processing of personal data relating to him or her by a statement or by a clear affirmative action?[54]

Q.III.2.a.ii.q Is the controller able to demonstrate that the data subject has consented to the processing of his or her personal data?

Q.III.2.b Processing on the Basis of a Contract (Article 6(1)(b) GDPR)

Q.III.2.b.i Is the processing of personal data necessary for the performance of a contract to which the data subject is party?

Q.III.2.b.ii Is the processing of personal data necessary in order to take steps at the request of the data subject prior to entering into a contract?

Q.III.2.b.iii Is the processing of each type of personal data involved necessary for the above-mentioned purposes?

Q.III.2.c. Processing on the Basis of Legal Obligation (Article 6(1)(c) GDPR)

Q.III.2.c.i Is the processing of personal data necessary for compliance with a legal obligation to which the service provider is subject?

Q.III.2.c.i.a. What legal provision does establish the obligation? Does it have a basis in Union or Member State law? Does Union or Member State law determine the purpose of the processing? [55]

Q.III.2.c.i.b. Does the law establish specifications for determining the type(s) of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing?

Q.III.2.c.i.c. If so, does the service provider ensure compliance with these specifications (e.g. by not providing for “free fields”)?

[54] For example, bypassing an informative banner, or by checking-in through the electronic travel card etc.
[55] In replying to this question it will turn useful the preliminary analysis carried out as per paragraph 4.a.

Q.III.2.c.i.d. If the law does not itself specify what data may be collected: Is the processing/are the data really necessary to meet the obligation?

Q.III.2.c.ii Does/may the intended use of the product or service require/involve the processing of personal data that is necessary for compliance with a legal obligation which has a basis in Union or Member State law and to which the user of the product or service is/may be subject?

Q.III.2.d Processing on the Basis of Vital Interests (Article 6(1)(d) GDPR)

Q.III.2.d.i Is the processing of personal data necessary in order to protect the vital interests of the data subject or of another natural person?

Q.III.2.d.ii What are the relevant vital interests?

Q.III.2.d.iii Is it necessary to rely on this criterion, or can the consent of the data subject be obtained?

Q.III.2.d.iv If the processing is based on the vital interest of another natural person: Is it necessary to rely on this criterion, or can the processing be manifestly based on another legal ground?

Q.III.2.e. Processing on the Basis of a Public Task (Articles 6(1)(e), (2)+(3) and 36(5) GDPR)

Q.III.2.e.i. Is the processing of personal data necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller?

Q.III.2.e.ii. Is the basis for the processing laid down by Union law or Member State law to which the controller is subject? What is the relevant legal provision?

Q.III.2.e.iii. Does the law establish specifications for determining the type(s) of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitation, the storage period and processing operations and processing procedures, including measures to ensure lawful and fair processing?

Q.III.2.e.iii.a. If so, does the service provider ensure compliance with these specifications (e.g. by not providing for “free fields”)?

Q.III.2.e.iii.b. If the law does not establish said specifications: Is the processing / are the data really necessary for the performance of that public task?

Q.III.2.e.iii.c. Does Member State law require the service provider to consult with, and obtain prior authorization from, the supervisory authority?

Q.III.2.e.iii.d. If so, has the service provider consulted with and obtained prior authorization from the competent supervisory authority?

Q.III.2.f. Processing on the Basis of Balancing of Interests (Article 6(1)(f) GDPR)

This legal ground is **not applicable** to a service provider that is a **public authority** and carries out the processing in the performance of its tasks. If the service provider is not a public authority, please reply to the questions below.

Q.III.2.f.i. Is the processing of personal data necessary for the purpose(s) of the legitimate interests pursued by the service provider or by a third party? More precisely: **Q.III.2.f.ii.** What legitimate interests of the service provider or of a third party are served by the processing?

Q.III.2.f.iii. What fundamental rights and interests of the data subjects are affected by the processing?

Q.III.2.f.iv. Is the right balance struck between these competing interests (i.e. are the legitimate interests of the service provider not overridden by the rights and interests of the data subjects)?

Q.III.3. Necessity and proportionality

Q.III.3.a. Is the intended personal data processing **necessary** to achieve the objectives pursued by the data controller? More precisely:

Q.III.3.a.i. Is/was the objective pursuable by means of processing of non-personal data? Is there a least intrusive means to achieve the same objective

Q.III.3.a.ii Is the data storage duration limited?

Q.III.3.a.iii. Is the amount of personal data collected limited to what is necessary?

Q.III.3.a.iv. Is the objective provided for by law in the pursuit of a public interest? What is the public interest at stake and why it makes it necessary to process personal data?

Q.III.3.b. Is the intended personal data processing **proportionate** in pursuing the objectives of the data controller? More precisely:

Q.III.3.b.i. Is access to personal data limited only to authorized persons?

Q.III.3.b.ii. How are data subjects' rights respected (i.e. right of access and portability, right to rectify, erase, object, restriction of processing)?

Q.III.3.b.iii. Are technical safeguards applied to personal data, such as pseudonymisation?

Q.III.3.b.iv. If personal data are transferred outside the European Union, under what safeguards the transfer is performed?

Q.III.4. Risks for personal data protection and other freedoms of the data subjects

Please describe if the data subjects run one or more of the following risks and how they could be affected.

Description of risk	Likelihood/impact of risk (Low/Medium/High)	Severity of the risk (Low/Medium/High)
Accidental or unlawful destruction of personal data		
Loss of personal data		
Alteration of personal data		
Unauthorized disclosure of, or access to, personal data		
Financial loss		
Discrimination		
Identity Theft		
Damage to the reputation		
Breach of professional secrecy		
Unauthorised reversal of pseudonymisation		

Other risks (please describe)		

If these risks should materialize, may they lead to physical, material or non-material damage? *Please describe*.

Q.III.5. Measures envisaged to address the risks

Please describe, for each of the identified risks, what measures are taken to address them.

	Description of risk	Countermeasures
Risk 1	Accidental or unlawful destruction of personal data	
Risk 2	Loss of personal data	
Risk 3	Alteration of personal data	
Risk 4	Unauthorized disclosure of, or access to, personal data	
Risk 5	Financial loss	
Risk 6	Discrimination	
Risk 7	Identity Theft	
Risk 8	Damage to the reputation	
Risk 9	Breach of professional secrecy	
Risk 10	Unauthorised reversal of pseudonymisation	
Risk 11	Other risks (please describe)	

Example of solutions: reduction of data collected; short retention period; destruction of data at regular intervals; security measures; staff training and guidance on the ToE; adherence to a certification mechanism or to a code of conduct; pseudonymisation of data; anonymisation of data; campaigns and measures to increase data subject awareness; easy opt-out for data subjects; agreements/contracts in place with external data controllers or processors, including data sharing agreements; consultation with internal/external stakeholders

Outcome of the PIA

Option 1 - The PIA is deemed acceptable: action plan

Countermeasure	Controller[56]	Difficulty	Financial Cost	Term	Progress

The scales below can be used to develop the action plan and monitor its implementation:

Criteria	Level 1	Level 2	Level 3
Difficulty	Low	Moderate	High
Financial Cost	Nil	Moderate	High
Term	Quarter	Year	3 years
Progress	Not Started	In progress	Completed

The wording below shows a way of carrying out the formal validation of the PIA

Validation of the PIA	On [date], [identity or function] validates the PIA in the light of the study conducted and the PIA report. The processing should allow [synthesis of stakes]. The manner in which it is planned to implement the legal requirements and treat the risks is deemed acceptable in view of these stakes. The implementation of the action plan as well as the continuous improvement of the PIA will be demonstrated. [Signature]

Option 2 - The PIA is not deemed acceptable: consult with the Data Protection Authority

[56] The controller here is the person/function in charge to apply/monitor the countermeasure.

When the high risks identified by the PIA cannot be fully tackled by the countermeasures, then the competent Data Protection Authority must be consulted by the data controller prior to starting the processing activities.