The BRIGHT project is co-founded by the EU's Horizon 2020 innovation programme under grant agreement No 957816

Ref. Ares(2020)8003973 - 30/12/2020

Boosting DR through increased communIty-level consumer engaGement by combining Data-driven and blockcHain technology Tools with social science approaches and multi-value service design

Deliverable D10.2 POPD-Requirements no. 2

Author(s): Giuseppe Raveduto (ENG), Vincenzo Croce (ENG), Elena Sartini (CEL); Andrea Iannone (CEL); Carmela Occhipinti (CEL)

The project Boosting DR through increased communIty-level consumer engaGement by combining Data-driven and blockcHain technology Tools with social science approaches and multi-value service design (BRIGHT) has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957816. The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the Innovation and Networks Executive Agency (INEA) or the European Commission (EC). INEA or the EC are not responsible for any use that may be made of the information contained therein.

Imprint

Title:	**POPD – Requirements no. 2**
Contractual Date of Delivery to the EC:	31/12/2020
Actual Date of Delivery to the EC:	31/12/2020
Author(s):	Giuseppe Raveduto (ENG); Vincenzo Croce (ENG); Elena Sartini (CEL); Andrea Iannone (CEL); Carmela Occhipinti (CEL)
Participant(s):	ENG, CEL,
Project:	Boosting DR through increased communIty-level consumer engaGement by combining Data-driven and blockcHain technology Tools with social science approaches and multi-value service design (BRIGHT)
Work Package:	WP10 – Ethics Requirements
Task:	NA
Confidentiality:	Confidential
Version:	1.0

Table of Contents

List of Tables

List of Acronyms and Abbreviations

AI	Artificial Intelligence
APC	Asociatia Pro Consumatori
ASM	ASM Terni S.p.a
BRIGHT	Boosting DR through increased communIty-level consumer engaGement by combining Data-driven and blockcHain technology Tools with social science approaches and multi-value service design
CA	Consortium Agreement
CEL	CyberEthics Lab. Srls
CEN	Centrica Business Solutions Belgium N.V. (Centrica)
COM	COMSENSUS, Komunikacije in Senzorika, DOO SI
Consortium	Means the consortium created by the execution of the CA
Coordinator	Means ENG
DoA	Description of actions
DOMX	DOMX PRIVATE COMPANY
DR	Demand Response
DuCoop	Nieuwe Dokken Cooperative CBVA
EC	European Commission
EDPB	European Data Protection Board
EMOT	Emotion Srl
ENG	ENGINEERING Ingegneria Informatica S.p.a
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation no. 679/2016
IMEC	IMEC
ISKRA	ISKRAMECO
Partner	Means the BRIGHT partners as indicated within the CA
Project	Indicates the present project
RES	Renewable Energy Source
SONCE	SONCE New Energy Ltd.
SUN	SunContract OÜ
TNO	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk Onderzoek
TUC	Technical University of Cluj-Napoca
VPP	Virtul Power Plants
WP	Work Package
WP29	Working Party 29
WVT	WATT+VOLT S.A

Table 1 List of Acronyms and Abbreviations

Executive Summary

The present deliverable **D10.2 – POPD - Requirement No.2** aims at providing the reader with the description of the measures that will be implemented by the Project (either at Partner and Consortium level) to protect and ensure the fundamental rights of personal data protection and privacy (articles 7 and 8 of the EU Charter of Fundamental Rights).

In this respect, the document will provide the countermeasures that will be adopted in case of performance of profiling activities based of personal data collected by the Partners for the purposes of the Project, as well as the declaration that the respect of the principle of data minimisation will be respected by simply processing data set that will directly pertain to Project research activities.

Furthermore in light of the fact that the protection of the two fundamental rights abovementioned requires the identification, design and implementation of ad hoc security measures, the deliverable will provide the description of the technical and organisational measures that will be adopted either at Partner and at Consortium level to protect the personal data processed for the purposes of the Project itself.

Finally the templates of the informed consent to be used to inform individual and gather their freely given consent to the data processing will be attached to the present document.

1. Introduction

Demand Response (DR) opportunities could potentially improve thanks to the increasing electrification of heat and transport and larger deployment of decentralized Renewable Energy Sources (RES). However, technology immaturity, regulatory fuzziness, and distorted business framework are limiting the extent of DR exploitation at residential consumer's level.

BRIGHT aims to put individual consumers at the centre of the process within a DR framework combining social-science driven user experience design and monetary and non-monetary incentives, in a participatory co-creation process. The framework for DR will leverage innovative technologies, including Digital Twin models, Virtual Power Plants (VPP) based on multi-layer blockchain smart contracts, and AI driven services for energy (power, heat, gas), mobility, health (comfort) and smart home. The tools, services, and the underlying enablers will be deployed in 4 demo sites in Belgium, Slovenia, Italy, and Greece, targeting around 1000 consumers in a variety of different community configurations. The validation will be complemented in the early stages by a lab-based validation in the Netherlands.

So as for the Project's objectives it is possible that Partners during the lifelong of the Project process personal data. In order to better identify the perimeter of scope of such data processing operations, CEL addressed the Partners with a specific questionnaire (the "**Data Protection Questionnaire**") whose template can be found in **Annex I – Data protection Questionnaire template**. In addition, in order to raise awareness on the issue, CEL alongside with the Coordinator organized an online webinar the 23rd of November 2020 to explain the content and the rational of the Data Protection Questionnaire.

As last remark, it is necessary to stress that the content of paragraphs included in section 6.1 (*Security measures at Partners' level*) has been directly provided by the relevant Partner, and CEL simply collected and incorporated the said content in the present document. In any case, each Partner (severally) remains the sole responsible on the accuracy, content and implementation of the security measures indicated therein.

1.1. Purpose

The purpose of the present document is to illustrate the procedures that will be followed and implemented when it comes to personal data processing, in particular with reference to (i) compliance with transparency and information obligations as provided within GDPR; (ii) compliance with the principle of data minimisation; (iii) definition of countermeasures to ensure that the essence of the fundamental rights of privacy and data protection are in any case respected in case of performance of profiling activities; and (iv) the security measures (to be intended in the broader term as possible) that will be implemented either at Partner and/or Consortium level to protect personal data object of processing activities.

1.2. Relation to Other Activities

The present deliverable should be read in conjunction with D10.1 – H Requirements no.1 regarding the informed consent procedure that will be followed by Partners when involving individuals in Project's research activities.

Moreover, in consideration to the importance of the principles and procedures illustrated in the present document, the same should be used as starting point whenever for Project's research reasons Partners will process personal data and/or start any specific research activity related to the Project.

1.3. Structure of the Document

The present document is composed by 5 sections divided in several paragraphs and sub-paragraphs. In general terms it is possible to say that for each section is provided an initial conceptual framework aimed at identify the applicable principles and guidelines, followed by paragraphs dedicated to the specific measures that will be implemented by the Partners and/or by the Consortium to ensure the compliance with the conceptual framework presented.

2 Potential data processing activities within BRIGHT

As explained in section 1 (*Introduction*), by answering to the Data Protection Questionnaire some of the Partners declared that they might process personal data during the life of the Project, as well as share the same with other Partners.

Against this backdrop, it is necessary to preliminary recall the meaning of the terms "personal data" and "processing", as provided in article 4 (1) and (2) of the GDPR, which are respectively "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*"; and "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

To better identify the perimeter of such personal data processing, Partners have been requested to answer considering whether or not they will carry out processing activities for the performance of the following macro-activities envisaged by Project's research:

- Project management (e.g appointing members of the advisory board);
- IT development (e.g. WP2, WP 4, WP5, WP6 and WP7 activities);
- WP3 activities;
- Pilots' activities;
- Dissemination, Communication, and Exploitation.

Considering the very early stage of the Project and provided that additional activities and/or scenario might arise during the Project execution, those activities or scenario will be analysed and the most adequate arrangements to ensure a lawful data collection and processing operations will be identified and implemented.

Moreover, in consideration to the early stage of the Project, Partners have been given the possibility to answer with "yes", "no", "maybe" or "N/A" (applicable towards those Partners that pursuant to the DoA are not supposed to perform the said activity).

2.1 Potential Data Processing flows

For the purpose of the present deliverable, after having assessed that Partners will process personal data, it results fundamental to define what might be the data processing flows. This in consideration to the fact that, by identifying who among the Partners will be a data controllers, and/or a data processors, it will be possible to identify which Partner will be responsible to implement technical and organizational measures aimed at secure the personal data collected and processed.

Therefore, among the questions submitted with the Data Protection Questionnaire, Partners were requested to answer whether or not they will share personal data with other Partners (or with third parties).

In general terms, the following are the potential personal data processing operations that might be undertaken by Partners during the duration of the Project:

- a Partner is processing personal data for the purposes of the Project, but it is not going to share such personal data with the Consortium or with any other Partner;
- a Partner is going to process personal data for the purposes of the Project, and it is going to share such personal data with one or more than one Partner;

- a Partner is going to process personal data for the purposes of the Project and it is going to share such data with the entire Consortium.

According to the potential data flows envisaged in points no.1 and 2, each Partner would be responsible for the relevant data processing operations, and each of them shall be required to adapt and customize the BRIGHT Privacy Notice and Informed Consent Form attached hereto in **Annex II – BRIGHT Privacy Notice and Informed Consent Form**. Partners involved shall also take into consideration the characteristics of the relevant data processing, identifying who is the data controller, whether or not there are more than one data controllers, whether or not there is a data processor etc., and execute an agreement that reflects such characteristics pursuant to articles 26 and 28 of GDPR (in this respect, please consider that a template of such agreement can be found in **Annex III – Data Processing Agreement template**). Moreover, each Partner is required to ensure the appropriate measures and safeguards concerning data storage and security, modifying it accordingly due to the possible sharing.

In light of the above, each Partner shall be responsible to collect and store the documents related to the data processing, which will be safeguarded by the responsible Partner and kept in a secure location until they are destructed or required by the EC/REA.

On the other hand, according to the data flow described in point no. 3, the relevant personal data will be shared with the entire Consortium, and will be processed on behalf of the Consortium (which will be qualified as data controller).

For the sake of clarity, in consideration to the definition of data controller as provided within GDPR, and the responsibility deriving from that, the means and the purposes of the data processing to be made a Consortium level shall be decided during a BRIGHT Management Board (which according to the article 6.3.1.1.1 CA is composed by one representative per Partner). Moreover, while the Consortium will be held responsible for the data processing only in case of adoption of a resolution by the Management Board, during the meeting of the Management Board each Partner will have the possibility to accept or not the relevant personal data as well as the allocation of responsibilities pertaining to the data processing of such data (details of these aspects shall be provided within the said resolution).

As a consequence, only those Partners who accepted the said personal data shall be held responsible, and shall determine who among them shall have to request the consent to, and shall inform the data subject about the processing operation, as well as it shall have to provide appropriate technical and organisational measures. However, it should be understood that in any case, any personal data shared with the Consortium shall be collected lawfully, and that the relevant sharing - Partner shall remain responsible for any processing operation that took place before the sharing of the data with the Consortium.

2.2 Consent as lawful basis for personal data processing

In order to lawfully perform any processing activities concerning a personal data, each Partner is compelled to identify the most appropriate legal basis to do so. In this respect, according to article 6 of the GDPR one of the possible applicable legal basis is "consent" which is defined as "*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*" (article 4 (11) GDPR).

In addition to the definition provided by the cited article, article 7 of GDPR identifies some additional requirements to be respected in order to determine the validity of the consent of the data subject:

- consent shall be informed: this means that the data subject should receive an appropriate and adequate quantity and quality of information on the activities to which he/she is

consenting (including, but not limited to a description his/her rights, benefits and implications etc), and such information as well as the consent, shall be given in plain and understandable language;
- the individual should be granted with an adequate length of time to consciously decide;
- consent should be provided in writing (or if the individual is not able to do so, it should be otherwise recorded);
- consent should be freely given;
- consent can be withdrawn;
- if consent is given in the context of a wider declaration, it should be clearly distinguishable, in an intelligible and easily accessible form.

2.3 Informed Consent Procedure

Against this backdrop, and provided that consent is identified as the most suitable lawful basis for the data processing, the relevant Partner before starting any processing activities shall have to (i) inform the relevant data subject by means of tailored privacy notice and (ii) gather his/her freely given consent.

In light of the above, before requesting to a data subject its consent, each BRIGHT Partner shall made available, and shall customize, to the potential data subject the template of the BRIGHT Privacy Notice attached hereto in Annex II – BRIGHT Privacy Notice and Informed Consent Form, providing for all the relevant information on the data processing. It is in any case understood that the relevant Partner should ensure that the data subject received the said information in an understandable and adequate way and has had a sufficient time frame to process it and give his/her free consent. Furthermore, considering that for achieving Project's objectives external advisory boards will be appointed by the Coordinator, a tailored information sheet (i.e invitation letter) and privacy notice will be distributed to ensure the compliance of GDPR also in this respect.

In order to assure that such information are properly delivered to the data subjects, it is advisable that the template included in this deliverable in Annex II – BRIGHT Privacy Notice are translated into the data subject's mother tongue. The information may be provided to participants either in hard copy or online.

In any case to facilitate the works of each Partner, the template of the BRIGHT Privacy Notice attached hereto will be available on Project's repository in a downloadable and editable format.

As an additional remark, please consider also that for dissemination purposes a Project's website will be launched, whereby it might be possible that personal data will be collected. If this were to be the case, a tailored privacy and cookies policies will be published on the website, and before collecting any personal data the consent of the relevant user will be requested.

Finally, please note that the Informed Consent Procedure so far described shall be read in conjunction with the content of deliverable D10.1 - H - Requirement No. 1 providing for the procedures and criteria that will be used to identify/recruit research participants alongside th informed consent procedures that will be implemented for the participation of humans in Project's research activities.

3 Data minimisation principle: conceptual framework

The principle of data minimisation is one of the key provision envisaged in GDPR; in this respect article 5 (1) lett. c) of GDPR provides that "*1. Personal data shall be: (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)*".

In other word, the EU legislator requires that data controller, as well as data processor, process only those personal data that are (i) sufficient (in terms of quality and quantity) to properly fulfil the purpose identified; (ii) rationally linked to the processing activities, i.e. are relevant; and (iii) limited in the quality and quantity to what is necessary to fulfil the purpose identified.

As last remark it is important to highlight that the principle of data minimisation must read in conjunction also with the other data protection principles provided in article 5 of GDPR (i.e. lawfulness, fairness, transparency, purpose limitation, accuracy, storage limitation, integrity and confidentiality and accountability).

3.1 Data minimisation principle applied to the Project

As already stated in other part of the present document, each Partner of the Project is committed to respect and ensure the respect of data protection rules and principles, including the principle of data minimisation.

Therefore, each Partner shall ensure that the processing operation that will be carried out during the Project (and for the benefit of the Project research) encompass only and exclusively the bare minimum of the necessary personal data. In other words, before to start any processing activities, each Partner should ensure that each items of the following checklist is ticked:

☐the personal data collected are those that are actually needed for the specified purposes of the data processing;

☐the quantity and quality of personal data collected is sufficient to properly fulfil those purposes;

☐a periodic review of the data held is conducted, alongside with a periodic and deletion of anything (i.e of those personal data) that are not necessary.[1]

[1] The checklist has been elaborated by the UK Information Commission Officer, and it is available for consultation at the following link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/

4 Profiling activities

According to the answers provided by Partners to question no. 6 ("*Will you perform profiling and/or tracking activities on the personal/sensitive data collected during any of the activities below …"*), it is possible that for the purposes of achieving Projects' objectives profiling activities on personal data might be conducted.

Therefore, it is worth recalling the relevant data protection regime, aimed at ensuring that the rights and freedoms of the individuals involved are safeguarded and not put in prejudice.

Indeed, article 4 (4) of GDPR defines profiling as "*Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*", entailing therefore processing activities which by nature are extremely pervasive and intrusive on individual's life.

Following the definition provided above, the activity of profiling relevant for the purpose of GDPR involves three elements:

(i) it has to be an automated form of data processing. In this respect it is important to bear in mind that the definition in re differs from article 22 of GDPR in the sense that profiling activities might be carried out not only "*solely*" by automated means, but also with the involvement of human intervention (whilst article 22 of GDPR makes refence only to automated means of processing);

(ii) it has to be carried out on personal data; and

(iii) the scope of the profiling is to evaluate a personal aspect about an individual[2].

By making reference to the abovementioned definition, and to the WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (the "**Guidelines**")[3] it results that according to GDPR there might be 3 different scenarios:

1. pure profiling activities;
2. decision making based on profiling activities;and
3. solely automated decision making, which falls within the scope of application of article 22 of GDPR.

Provided that a controller is performing (or intends to perform) profiling activities shall pay particular attention to implement those safeguards that shall ensure the compliance with GDPR provisions, and more in general the respect of the essence of the rights to personal data protection and privacy.

In practical terms, and by making reference to the Guidelines, the relevant controller, i.e the relevant Partner, (as well as the processor) shall:

a) first at all, consult the Guidelines and/or any other relevant recommendations or piece of legislation that might result applicable to the case at hand;

b) ensure that the right of information is effective. In this respect, and to comply with the general principle of transparency, the controller shall explain in an intelligible way the

[2] Article 29 Data Protection Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", page 6 and 7, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 .

[3] Article 29 Data Protection Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

process, procedures, ratio and rationale of the means used to perform profiling activities. This is particularly relevant whenever the activities fall within the scope of application of article 22 of GDPR. Consequently, as the same Guidelines suggests, visual representation of the algorithm or of the profiling activities envisaged, can be used as support to address and comply with the obligation of transparency and information. Therefore, just the indication of a technical/mathematical explanation of the profiling operation will result not sufficient to meet the transparency obligation as set forth within GDPR;

c) identify the most suitable lawful basis. In this respect, provided that consent (article 6. 1 lett. a) has been identified as the most suitable and appropriate, the relevant data subject shall have the possibility to not grant his/her consent to the profiling activities, while he/she gives the consent to the data processing. In other word, an overcomprehensive consent box would result in breach of GDPR. In addition, "*data subjects should have enough relevant information about the envisaged use and consequences of the processing to ensure that any consent they provide represents an informed choice*"[4];
d) ensure that the relevant data subject is actually in the position to exercise his/her rights to object (to the processing and/or the profiling activities), to access to his/her personal data object of the profiling activities (in this respect, the controller might consider to implement a specific system to ensure the data access), as well as to rectify his/her personal data;
e) ensure that the obligations set forth in article 22 of GDPR in case of profiling activities based on solely automated decision making are duly complied with. In this respect, the controller shall ensure a form of human intervention in the process, as well as a periodic external check of the algorithm used as well as of the procedures adopted. External audits might therefore extremely useful also to evaluate whether or not other GDPR principles (such as for example data minimisation, or data storage limitation) are effectively respected.

[4] Ibid.

5 Security measures to protect personal data and privacy rights: conceptual framework

Having considered the above, it is worth noticing that the EU legislator within GDPR has provided for a set of principles and rules aimed at regulating the processing of the personal data in the most complete and comprehensive way as possible, including also provisions concerning the protection and the security of the personal data during all the processing stages (from the development and design of a new technology, to the data storage policies to be implemented to avoid data breach or intrusion).

Indeed, given the very broad meaning of the term "processing" the provisions envisaged within GDPR are not simply referred to the material activities regarding the collection and the analysis of the personal data, but rather they refer to any kind of activity or set of activities having as subject matter personal data. In this respect, what it is important to bear in mind is that when we are talking about the provisions concerning the security of the personal data, such provisions are not simply referring for the measures *per se*. On the contrary, the said provisions shall be measured with their ability to effectively ensure the protection of those rights listed within GDPR, or in other fundamental charts, that an individual has in relation to the processing of his/her personal data.

It is in this light that should be read the concept of security of personal data, firstly provided in article 5, letter f) of GDPR, as the principle of "integrity and confidentiality" of the data processing, pursuant to which personal data should be *"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*".

The definition of the appropriate technical and/or organizational measures to be implemented is not provided nor described in detail within the legislative text[5]. In fact, the EU legislator rather than providing strict standards preferred to try to better explain these concepts in articles 25 (*Data Protection by design and by default*) and in article 32 of GDPR (*Security of processing*), suggesting possible techniques, but at the same time leaving some space of manoeuvre to the responsible organizations. These, before implementing any measures might consider the most suitable and appropriate ones, having in mind that the measures to be implemented shall effectively protect the data processed. It is in fact possible to say the GDPR adopted a risk-based approach, whereby the relevant organization should assess the security risks connected to the processing, combining it with the state of the art as well as the costs of implementation.

In particular, article 25 of GDPR introduces the concepts of "privacy by design" and "privacy by default", both aimed at ensuring that either during the development, and on later stage, new technologies (or old ones revised in light of GDPR) shall implement features aimed at protecting the privacy of the individuals whose data are used and processed within the technology. In particular, the controller,

"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

[5] The same EDPB within Guidelines 4/2019 on Article 25 Data Protection by Design and by Default adopted the 13th of November 2019, section 2.1.1, paragraph 9, page 6 stated that "*A technical or organisational measure can be anything from the use of advanced technical solutions to the basic training of personnel, for example on how to handle customer data. There is no requirement to the sophistication of a measure as long as it is appropriate for implementing the data protection principles effectively*".

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.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. 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."
Pseudonymisation (to be understood as a method to "hide and separate" the identity of an individual from other element derived from a personal data), minimization (either in terms of data quantity and quality, which in any case should be measured having considered the processing purposes) as well as the principle of accountability should be considered as key elements to be implemented and ensured when it comes to protect personal data.
In addition, recital 78 of GDPR (which even if it has not binding force, can in any case provide some guidance) also makes reference to the necessity to ensure the transparency of the processing operations "(…) *enabling the data subject to monitor the data processing, enabling the controller to create and improve security features (…)*".
Besides article 25 of GDPR, Section 2 of the same legislative text concerns the security of personal data. In particular, as mentioned above, article 32 of GDPR refers to "*technical and organizational measures*" as means, instruments to be implemented, to ensure the protection and security of personal data processed. However, here the obligation to implement such measures is either on the data controller and on the data processor, which might implement measures able to ensure:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[6]

As also stated in recital 83 of GDPR which even if it has not binding force, can in any case provide some guidance), all the said measures shall be aimed at avoid "(…) *accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage*".
In particular, even if within GDPR there are not example of what could be a pseudonymisation technique, a glance can be derived by reading the ENISA report[7], whereby the EU agency provides some examples of the best practices so far developed.
Moreover, even if not specified in the above list, another possible technical measure to ensure the security of the data processing is the anonymization. Pursuant to recital 26, which, once again, has not a binding force but nevertheless might provide guidance in interpreting GDPR, anonymous information are "*information which does not relate to an identified or identifiable natural person or*

[6] Emphasis added.
[7] European Union Agency for Cybersecurity (ENISA), Pseudonymisation techniques and best practices. (2019) - https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes".

5.1 Security measures: BRIGHT framework

Against this backdrop, within the following sections, it will be illustrated (i) the measures at Consortium level to ensure the protection of personal data in terms of monitoring activities and principles to be respected (also considering certain specific activities, such as Project's website development and management); (ii) the procedure to be followed to publish/upload a document providing personal data in the Project shared environment; (iii) the procedures and the safeguards adopted to ensure the protection of personal data in case of transfer to third countries; and (iv) the technical and organisational measures that each Partner will implement to protect personal data to be processed during the Project.

5.1.1 Technical and organizational measures at Consortium's level

In general terms, the Consortium considers one of its priorities to ensure the compliance with the highest ethical, data protection and privacy standards aimed at guarantying the integrity and the confidentiality of the personal data to be processed, as well as privacy rights.

Moreover, provided that the Consortium might be identified as data controller (pursuant to the conditions explained above in section 2.1 (*Potential Data Processing Flows*)), the same shall respect, inter alia, those data protection principles concerning: (i) the minimization of the quantity and quality of the personal data processed; (ii) the implementation of pseudonymization techniques, or when it possible without jeopardizing the scientific research, anonymization techniques; (iii) the respect of the principle of the "need to know" with reference to the access of the personal data collected, as well as (iv) the respect of the shorter data storage policy as it might be possible.

Without prejudice to the above, and to the sections concerning the technical and organisational measures to be adopted by each Partner, in the following subparagraphs it will be illustrated the measures so far implemented in agreement with all the Partners to comply with the principles set forth in article 5 paragraph 1, letter f) of GDPR with reference to some specific activities.

6 Website

For the purpose of dissemination activities, the Consortium will launch a Project website. In order to comply with all the transparency obligations as set forth within GDPR, whenever the website will require the collection (or processing) of personal data, it will be required to the relevant user to check a box to verify that the same is granting its consent to collect its information (name, email address and optionally phone number). To this extent, a tailored privacy and cookies policy will be published on the website to transparently and intelligibly inform the web user about the data processing operations. The data controller of the website will be ASM.

As per the protection of the personal data to be collected from a user, as well as the personal data of the personnel of the Partners, which might be published, the website will be host and will use servers hosted in the headquarters of Sistematica S.p.A in Via D. Bramante, 43 - 05100 Terni (Italy), that proved their commitment and security standards.

Furthermore, pseudonymisation measures will be implemented with reference to the data stored, and the collection of the data will be reduced only to those personal data strictly necessary for the dissemination of Project's results, events, or works.

Additional recommendations that might be implemented to ensure the protection of the website include the following:

Basic precautions

- implement the Transport Layer Security ("**TLS**") protocol (replacing the deprecated predecessor Secure Sockets Layer) on all website pages, using only the most recent versions and checking its correct implementation;
- make the use of TLS mandatory for all authentication pages, form pages or pages on which non-public personal data is displayed or transmitted;
- limit the communication ports strictly necessary for the proper functioning of the installed applications;
- restrict access to administration tools and interfaces to authorized persons only. In particular, limit the use of administrator accounts to the teams in charge of IT, and only for those administration actions that require it;
- if cookies that are not necessary for the service are used, obtain the consent of the Internet user after informing him/her and before placing the cookie;
- limit the number of components implemented, monitor and update them.

*What **not** to do*:

- to transmit personal data in a URL such as identifiers or passwords;
- use unsecured services (plain text authentication, plain text feeds, etc.);
- use servers as workstations, such as for browsing websites, accessing email, etc.;
- place databases on a server directly accessible from the Internet;
- use generic user accounts (i.e. shared between several users).

6.1 Security measures at Partners' level

For the sake of clarity, the content that follows have been communicated by the Partners to CEL by the time of submission of the present deliverable (i.e., month 2 of the Project, December 2020) either (i) by directly providing the relevant paragraph or (ii) by transposing the answers to the set of questionnaires related to data processing during the Project that have been submitted by CEL to the Partners.

It is in any case understood that besides the specific measures that the relevant Partner shall have to comply with (as they are described therein), when personal data are shared among Partners, the involved Partners shall define their roles in the processing (data controller, data processor, joint controllership) as well as the relevant additional measures that they might be required to implement to protect the personal data concerned, alongside with the execution of a data processing agreement in the form and substance equivalent to the one attached in Annex III – Data Processing Agreement template.

As a last remark, it should be noted that provided that a Partner is processing one of the category of personal data falling within the scope of application of article 9, paragraph 1 of GDPR, the same shall ensure a higher level of security of the personal data.

6.2 Data transfer

According to the answers provided by some Partners it results that some of them might share (i.e. transfer) personal data to entities outside the Consortium. Without prejudice to the fact that before to perform such activity the relevant Partner shall ensure to have identified all the relevant and necessary legal instrument to do so (including but not limited to, the execution of a data processing agreement, as well as the potentially necessary authorisation by the Consortium or by another Partner), the involved Partner:

- shall ensure to have identified a valid legal basis (pursuant to Chapter 5 of GDPR) to perform the said transfer, and it shall have clearly established the roles played by the entities involved (controller – processors; joint controllership); and
- shall also evaluate whether or not the recipient of the personal data is located outside the European Economic Area or not. If this is the case, the recipient shall provide the Partner (which shall provide the same information and documentation to the Consortium) with all the information attesting its compliance with GDPR, in particular with reference to the identification of appropriate and adequate measures of protection of the personal data object of the transfer.

6.2.1 ENG

Technical measures: The tools and processes to be used will be selected according to the nature of the data.
Organizational measures: Engineering follows a specific internal process for privacy management under GDPR. The process defines the governance structure, roles, risks, impact evaluation, and procedures related to the protection of personal data.
Encryption techniques: Usage of widely recognized encryption standards (e.g. AES for symmetric-key encryption and RSA for public-key systems) and tools (e.g. GnuPG).
Anonymisation techniques: Considering techniques such as noise addition, substitution, or data aggregation. Anonymisation techniques will be applied prior to data transfer, if needed.
Pseudonymisation techniques: Pseudonymised personal data will be considered to be information on an identifiable natural person.

6.2.2 TUC

Technical measures: Access control and authentication; Server/Database security; Workstation security; Physical security;
Organizational measures: Access control policy; Roles and responsibilities; Security policy and procedures for the protection of personal data;
Encryption techniques: Password protection
Anonymisation techniques: Data Aggregation
Pseudonymisation techniques: Masking

6.2.3 IMEC

Technical measures: storage on secure private cloud infrastructure hosted on premise.
Organizational measures: only researcher directly involved in BRIGHT will get access to the data
Encryption techniques:
Anonymisation techniques: we will not directly collect data ourselves, but use data from the pilot owners which will probably be anonymised already. If not, we will of course never disclose any personal/sensitive data publicly.
Pseudonymisation techniques:

6.2.4 COM

Technical measures: To be defined
Organizational measures: To be defined
Encryption techniques: To be defined
Anonymisation techniques: To be defined
Pseudonymisation techniques: To be defined

6.2.5 SONCE

Technical measures: Encryption techniques and Pseudonymisation techniques for separating personal data from identification factor.
Organizational measures: Permission structures, that data cannot be access by all, only persons directly involved in the project activities.
Encryption techniques: Standard encryption for data access protection, additional protection for hashing passwords to be stored in databases, 2 Factor Authentications where possible.
Anonymisation techniques: Hashing of some particular data, anonymisation procedures in the process of data transferring to Data Warehouse.
Pseudonymisation techniques: To be define

6.2.6 ISKRA

Technical measures: Not decided yet.
Organizational measures: Not decided yet.
Encryption techniques: Not decided yet.
Anonymisation techniques: Not decided yet.
Pseudonymisation techniques: Not decided yet.

6.2.7 EMOT

Technical measures: Access control and authentication; Server/Database security; Workstation security; Physical security;
Organizational measures: Access control policy; Roles and responsibilities; Security policy and procedures for the protection of personal data;
Encryption techniques: Password protection
Anonymisation techniques: Data Aggregation
Pseudonymisation techniques: Masking

6.2.8 TNO

Technical measures: Two storage options will be considered (after consulting consortium partners and project's DMP): *Option 1: SharePoint Online* Information is stored in Microsoft's SharePoint Online service. The data is located within the EU (Ireland and the Netherlands). Access to the information is possible worldwide based on a TNO account or a TNO partner account, but always on the basis of Multi Factor Authentication. Microsoft offers standard features to ensure the confidentiality, integrity and availability of the information. In addition, TNO makes a daily back-up of the information to a service in the Amazon S3 Cloud, also within the EU. Both for SharePoint Online and for the backup use is made of encryption 'in transit' and 'at rest'. *This option is typical for all project related information, unless otherwise specified (see below).*

Option 2: Sharepoint in TNO Data Center Information is stored in the SharePoint service of TNO. The data is located in one of the two data centres contracted by TNO in the Netherlands. The equipment installed in these data centres is owned by TNO and is managed exclusively by TNO. Access to the information is possible worldwide based on a TNO account from the TNO network, or via TNO telecommuting facilities based on Multi Factor Authentication. TNO offers standard facilities to safeguard the confidentiality, integrity and availability of the information, including at least daily backup of the information to the data centre other than where the service itself is active. *This option will be considered for personal (pseudoanonymized) data that may be collected during WP3 activities (and potentially pilot activities after consultation with consortium partners).* It remains to be seen whether we would need to use software for processing (personal) data that is not provided by TNO on actual TNO servers. If indeed this is to be the case we will evaluate and arrange for a processor agreement with the software supplier.
Organizational measures: Apply access rights controls; in particular access to personal (pseudoanonymized) data will be limited to the researchers "on need-to-know basis"; when sharing between consortium partners, project's DMP is applicable; the project's repository (Microsoft Teams) will also be used according to the guidelines as specified by the project coordinator. Only reports and deliverables specified as public will be shared on website and other communication channels as identified by the project's communication plan. Open software and tools will be shared via platforms are identified by the project's exploitation guidelines (such as for example GitHub[8]).
Encryption techniques: When personal data are transmitted electronically to a receiver outside TNO, the data can be encrypted using the SURF File Sender[9]. Unless otherwise explicitly specified the project's repo facilities will be used.
Anonymisation techniques: For IT development and whenever possible for social studies we will use anonymisation techniques such as *randomization* or *generalization* according to opinion 05/2014 on Anonymisation Techniques as a result of the working party on data protection of individuals (see also article 29). Specifically, for social studies whenever anonymized data are not available or suitable, data will be pseudoanonymised (see also below)
Pseudonymisation techniques: *Encryption with secret key*; for social science studies data through which a person can be identified from the dataset will be removed and stored with a key in a separate password protected data file that only the researchers working with the data will have access to.

[8] https://github.com/
[9] https://www.surf.nl/en/surffilesender-send-large-files-securely-and-encrypted

6.2.9 CEN

Technical measures: right to be forgotten is provided, according to GDPR compliant process.
Organizational measures: Chinese wall principle
Encryption techniques: all data is encrypted
Anonymisation techniques: where applicable
Pseudonymisation techniques: where applicable

6.2.10 ASM

Technical measures: 2 databases
Organizational measures: ASM manages different tools which process personal data for its business objectives (e.g., energy system, hydro system, gas network ...); those are already managed according to best practices, nevertheless we will refer only to the infrastructure that will be used in BRIGHT project (i.e., near real time smart meters and related data gathering infrastructure).
Encryption techniques:
Anonymisation techniques:
Pseudonymisation techniques:

6.2.11 DuCoop

Technical measures: access to personal/sensitive data is limited with access restriction based on two-factor authentication (OAuth2 protocol).
Organizational measures: DuCoop has 5 employees, who will be working tightly together also in the context of the Bright project. No organisational measures are therefore taken with regards to data or data access.
Encryption techniques: encryption of the data, stored in an influxDB database on Amazon S3 servers, happens at rest and at transit by AWS itself, with security policies described here: https://aws.amazon.com/compliance/data-center/controls/.

Anonymisation techniques:
Pseudonymisation techniques: the apartment numbers, linking inhabitants to their energy and water use, will be replaced by a random code when data is processed and/or transferred to partners other than the data processor and controller.

6.2.12 CEL

Technical measures: Data are collected and stored by using the CEL IT infrastructure, that is compliant to security standards.
Organizational measures: Personal data of BRIGHT partners involved in the project activities are shared internally to the consortium if and only if it is strictly necessary for the purpose and objectives of the research activities. In case of special public events, if personal data are coming from external persons (participating as volunteers having previously granted consent) these are not shared and will be permanently deleted after the end of the project. In general, persons provide personal data if and only if they: 1) participate on a voluntary basis; 2) are properly informed; 3) accept and provide explicit consent to the treatment of personal data. In principle, for the submission of questionnaires and for providing the subject with a courtesy summary of the submitted data, the most common example of personal data collected are email addresses.
Encryption techniques: at the time of the submission of the deliverable it has not been defined yet define the applicable technique. However, in the event it will be necessary, a dedicated paragraph will be inserted in the data management plan to be submitted at month 6 of the Project (i.e. April 2021).
Anonymisation techniques: Any personal data contained in questionnaires will be aggregated in order to be anonymised.
Pseudonymisation techniques: at the time of the submission of the deliverable it has not been defined yet define the applicable technique. However, in the event it will be necessary, a dedicated paragraph will be inserted in the data management plan to be submitted at month 6 of the Project (i.e. April 2021).

6.2.13 DOMX

Technical measures: - We use encryption and/or pseudonymisation where it is appropriate to do so. - We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. - We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy. - When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.

Organizational measures: - We understand the requirements of confidentiality, integrity and availability for the personal data we process. - We ensure that any data processor we use also implements appropriate technical and organisational measures. - We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design. - We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes. - We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals. - We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.
Encryption techniques: We employ encryption techniques when storing sensitive information like user passwords/ emails in the databases managed by our company. More specifically, we use the bcrypt password-hashing function that is based on the Blowfish cipher.
Anonymisation techniques: We user Anonymisation when required to share collected data with our list of collaborators. We make sure that no direct access to stored data is offered to any entity, but we only share limited copies of collected data, where personal information is deleted or masked. Through this process, the original personal information cannot be restored, thus such data is out of scope of the GDPR.
Pseudonymisation techniques: We implement the Tokenization Pseudonymisation technique, by separating personal data from non personal data that are stored in company servers. Personal data are kept in a separate file that is not stored on the web, but only locally at the company's premises and is not accessible by unauthorized users. This file links the personal data per subject with the stored data through a unique identification token, which has no extrinsic or exploitable meaning or value. We keep the rest non-identifiable data fully visible for processing and analytics while sensitive information is kept hidden in the separate file.

6.2.14 APC

Technical measures: N/A
Organizational measures: N/A
Encryption techniques: N/A
Anonymisation techniques: N/A

Pseudonymisation techniques: **N/A**

6.2.15 WVT

Technical measures: Not decided yet.
Organizational measures: Not decided yet.
Encryption techniques: Not decided yet.
Anonymisation techniques: Not decided yet.
Pseudonymisation techniques: Not decided yet.

6.2.16 SUN

Technical measures: We will separate personal data from identifier with pseudonymisation and anonymisation techniques.
Organizational measures: Separate folders that cannot be accessed by others who are not directly involved in personal data processing.
Encryption techniques: Standard encryption for data access protection, additional protection for hashing passwords to be stored in databases, 2 Factor Authentications where possible.
Anonymisation techniques: Hashing of some particular data, anonymisation procedures in the process of data transferring to Data Warehouse.
Pseudonymisation techniques: TBD

7 Conclusions

The aim of the present deliverable is to set the procedures, as well as to identify the security measures, that will be implemented by Partners during the life of the Project to ensure compliance with GDPR, and more in general to ensure an adequate and appropriate protection of the fundamental rights to privacy and personal data protection.

For this reason the document has been drafted including some conceptual framework to which the same Partners can make reference in case of doubt (without prejudice to the possibility to always contact the Coordinator or CEL), as well as more "practical" parts whereby Partners, directly, provided for the specific measures that they will implement to protect personal data.

Without prejudice to the above, it should also be noted that in consideration to the early stage of the Project, at the time of the submission of the present deliverable (i.e. month 2 of the Project, December 2020), it is possible that not all the possible countermeasures/procedures have been already identified by the relevant Partners. Therefore, considering that at month 6 of the Project (i.e. April 2021) will be released the Project data management plan, potential deviations or changes occurred in the time being will be duly reflected in the said document.

As last remark, it should also be considered that the present deliverable should be read in conjunction with deliverable D10.1 – H-Requirement no.1 regarding the criteria and the recruitment procedures that will be implemented by Partners when involving human beings in Project's activities.

References

- European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default adopted the 13th of November 2019 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf;
- European Union Agency for Cybersecurity (ENISA), Pseudonymisation techniques and best practices. (2019) - https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices;
- ENISA, "Infographic – Cybersecurity in Healthcare", available at https://www.enisa.europa.eu/topics/wfh-covid19/enisa_ehealth_infographic_pdf;
- Regulation (EU) 2016/679 of the Parliament of the European Union and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=it;
- Working Group 29, Guidelines on Consent under Regulation 2016/679, of the 6th July 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051;
- Working Party 29, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053;
- UK Information Commission Officer, Principle of data minimisation, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/.

Annex I – Data Protection Questionnaire

Ethics & Data Protection Questionnaire

With reference to the BRIGHT Project, CyberEthics Lab. ("**CEL**") has been appointed to assist You in relation to the compliance with the ethics, data protection, and privacy requirements. To this extent, we kindly ask you to answer to the following questionnaire (by checking the relevant answer) concerning which kind of data and/or information you are currently, and/or you will be, using, managing, generating (or more in general processing) during the Project lifetime. In particular, in consideration to the complexity of the Project, please take note of the following division in macro-categories of the activities to be performed over the course of the Project:

- Project management (e.g appointing members of the advisory board);
- IT development (e.g. WP2, WP 4, WP5, WP6 and WP7 activities);
- WP3 activities;
- Pilots' activities;
- Dissemination, Communication, and Exploitation.

In this respect, we kindly ask you to answer the following questions, providing an answer for each aforementioned category of activities. If, as a Partner, you are not going to perform a specific activity please "tick" N/A. Furthermore, due to the early stage of the Project, if you are not sure whether or not you are going to perform a certain activity, or for a specific activity you are not sure if you will use data, you can also answer with "Maybe".

To facilitate your analysis, please make reference to the following definitions:

TERM	**DEFINITION**
Personal Data	Any information relating to an identified or identifiable natural person. In particular an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Sensitive Data	Sensitive Data are Personal Data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Data Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

	disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Technical and Organizational measure to protect personal data	Any measure designed and implemented to ensure the protection and security of the personal data collected by a controller and/or processor.
Pseudonymisation	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person
Controller	Means 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
Processor	Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
Data transfer	Means any activities that entail giving access, sharing, transferring or otherwise making available personal data collected/processed by a controller or a processer to another controller or processor.

Please provide below the company name and an email address of the person who is going to answer the questionnaire to use as a relevant point of contact for the purposes of the present questionnaire:
Company:
Email address:
DPO contact (if present):

1. In order to perform the activity selected below during the Project, will you recruit/involve individuals?				
	YES	**NO**	**MAYBE**	**N/A**
Project management (External boards, etc.)				
IT development				
WP3 activities				
Pilots' activities				
Dissemination, Communication and Exploitation (workshops, events, etc.)				

1.a. Provided that you answered the previous question with 'yes' or 'maybe', please provide details (e.g.: Will you recruit individuals belonging to your personnel, or external to your company? How will you approach them?

2. In order to perform the activity selected below during the Project, are you going to process personal data?				
	YES	**NO**	**MAYBE**	**N/A**
Project management (External boards, etc.)				
IT development				
WP3 activities				
Pilots' activities				

Dissemination, Communication and Exploitation (workshops, events, etc.)				

3. In order to perform the activity selected below during the Project, are you going to process sensitive data?

	YES	NO	MAYBE	N/A
Project management (External boards, etc.)				
IT development				
WP3 activities				
Pilots' activities				
Dissemination, Communication and Exploitation (workshops, events, etc.)				

4. Will you process personal/sensitive data of a minor or of an incapacitated person during any of the activities below?

	YES	NO	MAYBE	N/A
Project management (External boards, etc.)				
IT development				
WP3 activities				
Pilots' activities				

Dissemination, Communication and Exploitation (workshops, events, etc.)				

5. Will you perform voice and/or video recording of individuals for Project purposes during any of the activities below?

	YES	NO	MAYBE	N/A
Project management (External boards, etc.)				
IT development				
WP3 activities				
Pilots' activities				
Dissemination, Communication and Exploitation (workshops, events, etc.)				

6. Will you perform profiling and/or tracking activities on the personal/sensitive data collected during any of the activities below?

	YES	NO	MAYBE	N/A
Project management (External boards, etc.)				
IT development				
WP3 activities				
Pilots' activities				

Dissemination, Communication and Exploitation (workshops, events, etc.)				

7. Will you re-use personal/sensitive data previously collected (so called "secondary processing") during any of the activities below?				
	YES	**NO**	**MAYBE**	**N/A**
Project management (External boards, etc.)				
IT development				
WP3 activities				
Pilots' activities				
Dissemination, Communication and Exploitation (workshops, events, etc.)				
7.a. Provided that you answered the previous question with 'yes' or 'maybe', please provide details on how you informed individuals about the possibility that their personal data might be reused for several purposes, and please clearly indicate the legal basis on which such processing is taking place (e.g.: Did you provide a privacy policy? Did you have a lawful ground to process those data?)				

8. Will you share/transfer the data collected/processed during any of the activities below with other BRIGHT Consortium Partners?				
	YES	**NO**	**MAYBE**	**N/A**
Project management (External boards, etc.)				

IT development				
WP3 activities				
Pilots' activities				
Dissemination, Communication and Exploitation (workshops, events, etc.)				

9. Will you share the data collected/processed during any of the activities below outside the Consortium?

	YES	**NO**	**MAYBE**	**N/A**
Project management (External boards, etc.)				
IT development				
WP3 activities				
Pilots' activities				
Dissemination, Communication and Exploitation (workshops, events, etc.)				

10. Provided that you answered the previous question 9 with 'yes' or 'maybe', please provide details on the entity to which you will share the data, in particular indicating the country where such data will be transferred, and which is the relation with the receiving entity.

11. Provided that you will collect and process personal/sensitive data, for how long are you going to store it? (so called 'data retention')

12. Provided that you will collect and process personal/sensitive data, where are you going to store it? On a cloud server? Which one? Will you use specific IT tools/solutions to process the data collected? If so, which?

13. Provided that you will collect and process personal/sensitive data, please provide the description of the:
Technical measures:
Organizational measures:
Encryption techniques:
Anonymisation techniques:
Pseudonymisation techniques:
that you will implement to protect the data collected and to processed, in particular from unauthorised access.

14. For the purposes of the Project, are you going to reuse results, data, or experiments already performed or gathered in other projects or activities?

Annex II – BRIGHT Privacy Notice and Consent Form

The following document shall be duly (i) adapted according to the activities to be performed and (ii) translated in the languages of individuals **prior** to their involvement.

Privacy Notice and Consent Form for [please insert the relevant activity]

As a part of the work of the BRIGHT project, the Consortium, is committed to conduct certain activities concerning [[please insert a brief description of the activities involving personal data processing].

In light of the above [insert the name of the Partner responsible for the activities] ("**[●]**") shall be the data Controller of your personal data. [insert the name of the Partner responsible for the activities] is committed to take its responsibility regarding the security and privacy of Personal Data very seriously (as well as the Consortium as whole) and is going to be transparent about the type of data it collects and how it is being handled.

Pursuant to article 5 of the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), the Processing of the Personal Data carried out for the performance of the research activities [please specify the activity] for to the purposes of the Project will be based on the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and accountability.

To this extent, please read the following Privacy Notice (hereinafter the "**Privacy Notice**") that explains how it will be processed and protected your personal data by the Controller.

Any term indicated in capital letter shall have the meaning attributed to it within the GDPR, or otherwise provided hereto. However, if you have any doubt, please feel free to ask any kind of clarifications to the person who is delivering you the present Privacy Notice.

Contact Details

If You would like to exercise your rights under GDPR, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your Personal Data, please feel free to contact the following email address: [Please insert the email address of Partner DPO or of representative of the Partner responsible for this data processing]

Data Controller

The Data Controller of your Personal Data will be [insert the relevant Partner name organization]. [Please indicate if there is a data processor other than the data controller]

Personal Data processing and lawful basis

The Controller will only process the Personal Data that you will voluntarily and directly decide to provide and/or disclose to the same in connection and/or related to the [please insert the

activities], such as, for example, your name, surname, professional details information, job title and experiences, pictures.

The lawful basis pursuant to which the Controller will process your Personal Data shall be your freely and informed consent to the data processing itself given by you by signing the present Privacy Notice. Please note that you are free to give your consent as well as to deny it (article 6, paragraph 1 letter a of GDPR).

Furthermore, the [insert the name of the responsible partner] may use your Personal Data to comply with its tax and other legal obligations, including in terms of invoicing, accounting and archiving (article 6, paragraph 1 letter c of GDPR).

Purpose of the data processing

The Processing of your Personal Data will be limited to the extent necessary to perform each and all the activities connected and related to [describe the activities]. This might include also the publication of your Personal Data on BRIGHT website when it will be deployed, however you can object to the same.

Any other further processing of your Personal Data will be excluded without your previous consent.

[Profiling activities: TBD according to the relevant scenario. Please note that this section is extremely important and that the greater the level of understandable details you provide the better!]

Please note that the Controller will conduct profiling activities on the personal data that will collect from you. In this respect such activities will be carried on for the following reason(s): [please specify]. In addition, the profiling will be undertaken with the following means [solely automated/with human intervention: please specify]. In addition, the following paragraph describe the functioning of the algorithm/process used to perform the profilin [please specify].

In any case, please be aware that you can object at any time to the profiling activities envisaged, but at the same time still agreeing on the personal data processing.

As last remark, please do not hesitate to contact us if you have any specific doubt, or queries in this respect.

Recipients of Personal Data

Your Personal Data may be accessed, for the purposes referred above by:

- partners of the Consortium and related employees and external consultants. A list of the partners belonging to the Consortium is attached hereto in Annex 1 – List of Partners;
- our shared environment service provider [please specify];
- subjects, bodies or authorities to which the Controller is obliged to communicate your Personal Data pursuant to any applicable law.

The Controller may also share your information with the European Commission or with competent legal an/or fiscal authorities for legitimate reasons.

Please note that for the purposes of publishing the works of the Project, it might be possible that Your Personal Data will be published on the Project's website. In this respect, please note that the server of the website is [please insert the relevant details] and it is located in [please insert the relevant details].

[Personal Data transfer to third countries: TBD depending on the specific case]
[Please be aware of the fact that the Personal Data that we collect might be transferred to [please specify the country and the name of the entity receiving the data and the reasons]. In this respect please consider also that the said transfer will rely on the following legal basis in full compliance with Chapter 5 of GDPR [please specify the legal basis, as well as the security measures that the recipient of the data will implement].
In any case, you can object at any time to the said transfer, and the same will cease immediately.]

Data Retention and data security
Those Personal Data processed for the purposes set out in section "Purposes of the data processing" will be kept for the time strictly necessary to achieve the purposes stated therein. The Controller will store your information for [insert the relevant timeframe] after the end of your participation, or [insert the relevant timeframe] after our last contact with you, or the retention period required by law, whichever is longest, and for the applicable statute of limitations period thereafter.
In any case, to ensure the best level of protection of your Personal Data we will apply all the best physical and logical security measures internally, and our servers are subscribed from the most established cloud providers and protected through state of the art security measures.
[Please specify where the data will be stored, paying particular attention in the case you use cloud services and data might be shared with third countries]

Data subject rights
Pursuant to the GDPR, you have a number of rights concerning the Personal Data we hold about you. If you wish to exercise any of these rights, please contact our Data Protection Officer using the contact details set out above.

- **The right to be informed.** You have the right to be provided with clear, transparent and easily understandable information about how we use your information and your rights. This is why we're providing you with the information in this Privacy Policy.
- **The right of access.** You have the right to obtain access to your Personal Data subject matter of the data Processing. This will enable you, for example, to check that we're using your Personal Data in accordance with the relevant data protection law. If you wish to access the information we hold about you in this way, please get in touch (please see section Contact Details above)**.**

- **The right to rectification.** You are entitled to have your Personal Data corrected if it is inaccurate or incomplete. You can request that we rectify any errors in information that we hold by contacting us (please see section Contact Details above)**.**
- **The right to erasure.** This is also known as 'the right to be forgotten' and, in simple terms, enables you to request the deletion or removal of certain of the Personal Data that we hold about you by contacting us (please see section Contact Details above). Please remember that it is possible that pursuant any applicable law you may not have all your personal data erased**.**
- **The right to restrict processing.** You have rights to 'block' or 'suppress' certain further use of your Personal Data. When processing is restricted, we can still store your Personal Data, but will not use it further**.**
- **The right to data portability.** You have the right to obtain your personal information in an accessible and transferrable format so that you can re-use it for your own purposes across different service providers. This is not a general right however and there are exceptions. To learn more please get in touch (please see section Contact Details above)**.**
- **The right to lodge a complaint.** You have the right to lodge a complaint about the way we handle or process your Personal Data with the relevant national Data Protection Authority**.**
- **The right to withdraw consent.** If you have given your consent to anything we do with your Personal Data (i.e. we rely on consent as a legal basis for processing your information), you have the right to withdraw that consent at any time. You can do this by contacting us (please see section Contact Details above). Withdrawing consent will not however make unlawful our use of your information while consent had been apparent**.**
- **The right to object to processing.** You have the right to object to certain types of processing. You can for example object to the publication of pictures taken of you within the context of a conference held concerning the Project.

Changes

Where appropriate, we will notify you of any changes to this Privacy Notice, by email.
This Privacy Notice was last updated on [•] /2020.

***

Provided that You read and understood all the above mentioned information, and provided that You had the possibility to raise doubts or questions and that you received all the relevant clarifications and answers to your questions, You now,

☐ accept

☐ refuse

to give your consent that the Controller will process your Personal Data in connection to the [insert the specific research activities involving the individual and his/her personal data] pursuant to the abovementioned terms and conditions.

Provided that You read and understood all the above mentioned information, and provided that You had the possibility to raise doubts or questions and that you received all the relevant clarifications and answers to your questions, You now, give your consent that the Controller might transfer your Personal Data outside the European Economic Area to:

[specify the recipient in the third country]
☐ accept
☐ refuse

pursuant to the abovementioned terms and conditions, as well as to the legal grounds indicated in section Personal Data transfer to third countries above, always bearing in mind that you have the right to object to any, or all, of the abovementioned data transfer.

Provided that You read and understood all the above mentioned information, and provided that You had the possibility to raise doubts or questions and that you received all the relevant clarifications and answers to your questions, You now,

☐ accept

☐ refuse

to give your consent that the Controller will perform profiling activities on your Personal Data in connection to the [insert the specific research activities involving the individual and his/her personal data] pursuant to the abovementioned terms and conditions.

Annex 1 – List of Partners

- ENGINEERING - INGEGNERIA INFORMATICA SPA
- UNIVERSITATEA TEHNICA CLUJ-NAPOCA
- INTERUNIVERSITAIR MICRO-ELECTRONICA CENTRUM
- COMSENSUS, KOMUNIKACIJE IN SENZORIKA, DOO
- SONCE energija d. o. o.
- ISKRAEMECO, MERJENJE IN UPRAVLJANJEENERGIJE, D.D.
- EMOTION SRL

- NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO
- CENTRICA BUSINESS SOLUTIONS
- ASM TERNI SPA
- DUCOOP
- CYBERETHICS LAB SRLS
- DOMX IDIOTIKI KEFALAIOUCHIKI ETAIREIA
- Asociatia Pro Consumatori
- WATT AND VOLT ANONIMI ETAIRIA EKMETALLEYSIS ENALLAKTIKON MORFON ENERGEIAS
- SunContract OÜ

Annex III – Data Processing Agreement template

Pursuant to article 28, par. 3 of GDPR, the present Annex III –Data Processing Agreement template provides for the template of a data processing agreement that shall be executed by and between a Partner in its quality of data controller and a Partner in its quality of data processor, which for the purposes of the Project, has to process personal data collected by the data controller.
For the sake of clarity, each Partner that intends to enter into the present agreement shall have to agree with the security measures that will be implemented to protect the personal data subject matter of the agreement itself.
As a final remark, each Partner shall have to request its internal legal department its green light before to execute any data processing agreement, as the present annex simply represents an useful template.

***

This Data Processing Agreement

By and between:
[name and corporate details of the data controller (hereinafter the "**Company**" or "**Data Controller**") from one side,

and

[name and corporate details of the data processor (hereinafter the "**Data Processor**", and together with the Data Controller, the "**Parties**")]

WHEREAS:

- The [•] acts as a Data Controller.
- The [•] wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter, "**GDPR"**).
By the execution of the present agreement, the Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS.

1) **Definitions and Interpretation**

Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:
"**Agreement**" means this Data Processing Agreement and all Schedules;
"**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of the Data Controller pursuant to or in connection with the [please describe the activity from which the personal data have been collected in first instance].;
"**Contracted Processor**" means a Subprocessor
"**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country applicable to the specific case;
"**EEA**" means the European Economic Area;
"**GDPR**" means EU General Data Protection Regulation 2016/679;
"**Data Transfer**" means:

- a transfer of Company Personal Data from the Company to a Contracted Processor; or

- an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

"**Subprocessor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2) Processing of [•] Personal Data

Processor shall:

- comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and
- not Process [•] Personal Data other than on the relevant Company's documented instructions
- The Company instructs Processor to process Company Personal Data.
- Processor Personnel
- Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

3) Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. A list of the security measures implemented is attached at the present agreement [please attach to the agreement the list of security measures].

In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

4) Subprocessing

Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorized by the Company.

5) Data Subject Rights

Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

Processor shall:

- promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and
- ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws
- inform Company of that legal requirement before the Contracted Processor responds to the request.

6) Personal Data Breach

Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7) Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

8) Deletion or return of Company Personal Data

Subject to this section Processor shall promptly and in any event within10 business days of the date of cessation of [please describe the activity involving the processing operations] involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

Processor shall provide written certification to Company that it has fully complied with this section within 10 business days of the Cessation Date.

9) Audit rights

Subject to this section 9, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors.

Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law

10) Data Transfer

The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data

General Terms

11) **Confidentiality.**

Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("**Confidential Information**") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

- disclosure is required by law;
- the relevant information is already in the public domain.

12) Notices

All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13) Governing Laws and Jurisdiction

This Agreement is governed by the laws of [please insert the applicable law].

Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of [please insert the applicable jurisdiction].

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.