"This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 769765."

Project acronym:	WellCo
Project full title:	Wellbeing and Health Virtual Coach
Call identifier:	H2020-SC1-2017-CNECT-1
Type of action:	RIA- Research and Innovation Action
Start date:	1 December 2017
End date:	30 November 2020
Grant agreement no. :	769765

D2.2 – Ethics, Gender and Data Protection Compliance Protocol

WP2:	WellCo Co-design
Due Date:	30/04/2018
Submission Date:	08/05/2018
Responsible Partner:	Gerencia de Servicios Sociales de Castilla y León, GSS
Version:	1.2
Status:	Final Version
Reviewer(s):	MONSENSO and HIB
Deliverable Type:	R: Report
Dissemination Level:	PU: Public

VERSION HISTORY

Version	Date	Author	Partner	Description
0.1	02/04/2018	**Mª Jesús Miján (EUC)**	GSS	Initial Draft Version
0.2	11/04/2018	**José Miguel Sánchez (GSS)**	GSS	Reviewed version
0.3	16/02/2018	**Benedicto Caminero (Steering Committee Member)**	GSS	Reviewed version
0.4	23-27/04/2018	**Margarita González (FastCyL), Torben Uhrenholt (SDU), Venet Osmani (FBK)**	FastCyL, SDU, FBK	Reviewed version
0.5	26-30/04/2018	**Nanna Iversen, Mads Frost (Monsenso), Inmaculada Luengo (PC), Paloma Jimeno (Steering Committee Member - QAS)**	MONSENSO, HIB	Reviewed version
1.0	02/05/2018	**Mª Jesús Miján (EUC)**	HIB	Reviewed version
1.1	04/05/2018	**Inmaculada Luengo (PC), Katarzyna Wac (UCPH)**	HIB, UCPH	Reviewed version
1.2	08/05/2018	**Mª Jesús Miján (EUC)**	GSS	Final version

Table of contents

List of figures

List of tables

Glossary

Acronym	Definition
GDPR	General Data Protection Regulation
APPD	Act on Processing of Personal Data
EU	European Union
EEA	European Economic Area
DDPA	Danish Data Protection Agency
VAT	Value added tax
DKK	Danish krone
BCR	Binding Corporate Rules
SCC	Standard Contractual Clauses
IDPA	Italian Data Protection Agency
IDPC	Italian Data Protection Code
DPA	Data Protection Act
AGPD	Agencia General Protección de Datos
GDPR	General Data Protection Registry
WP29	Working Party 29
RRI	Responsible research and innovation
DPIA	Data Protection Impact Assessment

Executive Summary

This document presents an overview of three essential dimensions to be taken into account when implementing the project activities: ethics, gender and data protection. Section I describes ethics considerations. Section II presents key elements to address gender issues in the project. Section III analyses the regulatory basis for data protection, providing specific guidelines to accomplish with. In particular, the Data Protection Compliance protocol covers the different countries involved in the trials (Spain, Italy, Denmark), including: a) a description of the different European level and national regulations involved; b) interpretation of the regulation framework for WellCo project; c) elaboration of a data protection compliance protocol adapted to the requirements of the project.

PART I: Ethics

1.1 Ethics considerations in WellCo

- The purpose of this deliverable is to guide – in accordance with the ethics self-assessment- how the research and trials will be conducted in compliance with fundamental ethical principles.
- Ethics/gender and Data Protection Compliance protocol will be carried on covering the different countries involved in the trials providing robust safeguards to ensure compliance with ethical standards and privacy protections and take account of the gender dimension.
- As declared in the proposal, WellCo research involves human participants: they are volunteers for social or human sciences research.
- All of them are able to give informed consent and are not vulnerable individuals.
- This research does not include children/minors. Also, it does not include neither patients nor healthy volunteers for medical studies.
- WellCo research does not involve physical interventions on the study participants.
- By contrast, it does include personal data collection and its processing, being considered sensitive personal data. WellCo is going to gather information related to ethnicity, biometrics (like Heart Rate), and health status, but not about sexual lifestyle or political opinion.
- Tracking or observation of participants is also considered in WellCo, due to the use of wearables by the participants is part of the project. Furthermore, machine learning techniques are going to be implemented in the WellCo platform, so the system can learn about the participants behaviours, as well as from the interaction with the end-users.
- Due to the fact that measurements for chronic disease risk vary depending on social determinants of health (SDH) – among others, socioeconomic position, ethnicity, gender, age and location - EHR will provide data from men and women of different ages in Denmark. This EHR data analytics also implies following the ethics guidelines, i.e. to conceal the identity of data owners, all data is anonymised.

1.2 Deliverables related to Ethics

Prior to award decision, WellCo project was requested to include a new WP, WP7, related to Ethics.

The 'ethics requirements' that the project must comply with are included as deliverables in this work package.

Table 1 - WP7 Description and deliverables

Work package number [9]	WP7	**Lead beneficiary** [10]	1 - HI-IBERIA
Work package title	Ethics requirements		
Start month	1	**End month**	36

Description of work and role of partners
WP7 - Ethics requirements [Months: 1-36] **HI-IBERIA** This work package sets out the 'ethics requirements' that the project must comply with.

List of deliverables					
Deliverable Number[14]	Deliverable Title	Lead beneficiary	Type[15]	Dissemination level[16]	Due Date (in months)[17]
D7.1	POPD - Requirement No. 2	1 - HI-IBERIA	Ethics	Confidential, only for members of the consortium (including the Commission Services)	12
D7.2	H - Requirement No. 3	1 - HI-IBERIA	Ethics	Confidential, only for members of the consortium (including the Commission Services)	12

Table 2 - Deliverables included in the WP7

Deliverable Number: D7.1

Deliverable Title: POPD - Requirement No. 2

Lead beneficiary: HI IBERIA

Due date: M12

Dissemination level: Confidential

Content: This deliverable should include

4.1. Copies of opinion or confirmation by the competent Institutional Data Protection Officer and/or authorisation or notification by the National Data Protection Authority must be submitted (which ever applies according to the Data Protection Directive (EC Directive 95/46, currently under revision, and the national law).

4.2. If the position of a Data Protection Officer is established, their opinion/confirmation that all data collection and processing will be carried according to EU and national legislation, should be submitted.

4.7. The applicant must explicitly confirm that the data used are publicly available.

4.8. In case of data not publicly available, relevant authorisations must be provided.

Deliverable Number: D7.2

Deliverable Title: POPD - Requirement No. 3

Lead beneficiary: HI IBERIA

Due date: M12

Dissemination level: Confidential

Content: This deliverable should include

2.3. Templates of the informed consent forms and information sheet must be submitted on request.

1.3 WellCo grant requirements and ethics

1.3.1 Pre-grant requirements

WellCo has fulfilled the pre-grant requirements, by informing in detail about the following issues.

- 2.1. Details on the procedures and criteria that will be used to identify/recruit research participants.
- 2.2. Detailed information on the informed consent procedures that will be implemented for the participation of humans.
- 2.5. How consent/assent will be ensured in cases where adults may have cognitive difficulties and thus may be unable to give informed consent.
- 2.6. Whether vulnerable individuals/groups will be involved. Details about the measures taken to prevent the risk of enhancing vulnerability/stigmatisation of individuals/groups.

This information was already sent to the European Commission during the process of award, and later on being part of the signed Grant Agreement. Moreover, the detail of these processes is included in D2.1 User Involvement Plan.

1.3.2 Post-grant requirements

The consortium of WellCo project will also fulfil the following post-grant requirements:

Requested from EU Commission	Compliance with WellCo project
Copies of opinion or confirmation by the competent Institutional Data Protection Officer and/or authorisation or notification by the National Data Protection Authority must be submitted (whichever applies according to the Data Protection Directive (EC Directive 95/46, currently under revision, and the national law).	Every partner will confirm to HI IBERIA, as leader of WP7, the compliance of this requirement, where applies. A detailed description of the requirements is presented in Part 3 of this report.
If the position of a Data Protection Officer is established, their opinion/confirmation that all data collection and processing will be carried according to EU and national legislation, should be submitted.	The position of Data Protection Officer is not yet defined.
The applicant must explicitly confirm that the data used are publicly available.	The WellCo project includes the delivery of an Open Data Management Plan in WP6, led by UCPH due to WellCo takes part in the Pilot on Open Research Data. This deliverable (D6.6) is a report which will regulate the data management plan, provided at the beginning of the project (Month 6) and updated at each review period (M24 and M36).

	Scientific publications will be shared in the Open Access Infrastructure for Research (OpenAire).
In case of data not publicly available, relevant authorisations must be provided.	Non-applicable due to the information stated above.

Table 3.- Protection of personal data

Requested from EU Commission	Compliance with WellCo project
Templates of the informed consent forms and information sheet must be submitted on request.	To fulfil this requirement, the following actions will be performed: 1º) For the end-users participation during the co-design phase, the EUC has elaborated and shared with the consortium a set of documents in English to offer participants at the earlier stage (cultural probes) to be adapted by every pilot site to their cultural aspects and target population, including: • Letter for participants • Informed consent for participants (Appendixes- Informed consent for participants) • Ethics Code for Professionals (Appendixes - Confidentiality and Professional Ethics Agreement) • WellCo description • WellCo leaflet 2º) FBK, SDU and GSS have adapted and translated the proposed text to comply with the regulatory and legal aspects of their respective countries. 3º) FBK, SDU and GSS have proceeded to ask, when needed, the necessary authorisations or informed to the correspondent regulatory entities (It was needed in Denmark, but not in Italy or Spain). 4º) The templates used in every pilot site are uploaded to the WellCo project repository (Alfresco) and annexed as APPENDIXES, thus available for the consortium, and will be submitted upon EC request.
Copies of ethics approvals for the research with humans must be submitted.	Hi Iberia will collect copies of the necessary ethics approvals for the research with humans from the partners and available in the project repository (Alfresco), ready to be submitted upon request.

Table 4.- Research with Humans

1.4 Coordination of ethical issues

Work package number [9]	WP7	Lead beneficiary [10]	1 - HI-IBERIA
Work package title	Ethics requirements		
Start month	1	End month	36

The lead beneficiary regarding ethical issues is Hi Iberia, due to it is the lead beneficiary for WP7.

Nevertheless, this leadership will be supported by the End users & Ethics Board (EUEB) as a joint structure and by the End Users Coordinator (EUC) as an individual organisational structure.

As stated in the project proposal:

- On the one hand, the leading entity Hi Iberia holds the responsibility of WP7, Ethics, being responsible for the compliance of pre and post-grant requirements.
- On the other hand, Ethics and gender aspects are ensured in the project by the End users & Ethics Board (EUEB) that will research and document the practices, ethics and requirements for personal data protection. These ethical factors will address the legislation available in the different countries involved in the project, and that could influence the future adoption of the service.

End Users & Ethics Board (EUEB) and EUC will coordinate the activities where end-users are participating and guarantee their implication and active participation in the project.

Based on them EUEB, led by the **End Users Coordinator (EUC),** will ensure they are compliant in the WellCo trials.

Common Informed consent for participants will be distributed in trials in Denmark (SDU), Italy (FBK) and Spain (GSS) as well as an Ethics code for professionals involved.

1.4.1 End users & Ethics Board (EUEB)

EUEB will be led by GSS, as the leading partner of the task T2.1. User involvement plan and ethics/gender/data protection issues.

Tasks to be performed by the EUEB:

- will research and document the practices, ethics and requirements for personal data protection in the project, including secure and privacy-ensuring data acquisition, analysis, storage and dissemination to different actors.
- will follow up all activities, developments and results in the project to ensure that they are complying with gender/ethics aspects and current regulation for data protection/privacy, liability and consumer protection.

1.4.2 End Users Coordinator (EUC)

End Users Coordinator (EUC)	**The EUC is responsible for the coordination between the technical progress and the integration with end users in the different pilots and along the evolution of the prototypes plan. The EUC is in charge also of ensuring the fulfilment of the agreed Ethical Commitments for the WellCo Project**

The role of EUC will be held by María Jesús Miján, **Head of Service for Elderly Care and Dependency Prevention in GSS.**

1.5 Committees by country

To get better management of ethical issues, respective Ethical Committees will be created in every country participating in test trials. They will also contribute to research of information regarding the compliance of ethics regulation in every country.

Every trial partner will gather and document the regulations on their countries.

The composition of these 3 Ethical Committees is as follows:

Leader: María Jesús Miján Serrano (GSS)	Responsible for the Danish pilot site: Dr. Torben Uhrenholt (SDU)
	Responsible for the Italian pilot site: Enrico Piras (FBK)
	Responsible for the Spanish pilot site: María Jesús Miján Serrano (GSS)

Table 5.- Composition of the Ethical Committee

In the project, the following indication was included: "The project protocols in each of the three countries where the test trials are implemented will be submitted for approval to their respective Ethical Committees".

In order to provide better management of the above statement, this Protocol establishes that instead of designing 3 protocols (one per country), it will be just one but approved by the 3 pilot sites.

Therefore, and in order to fulfil this commitment as it as stated in the proposal, the process will be implemented as detailed in the figure below:

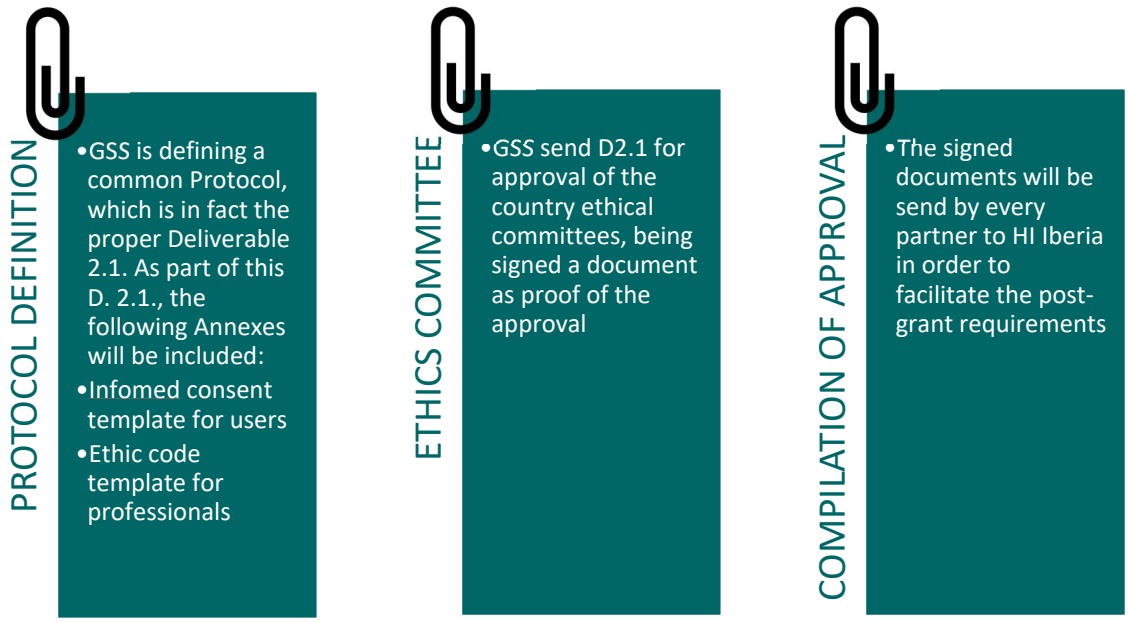

Figure 1 - Ethical approval process agreed by the WellCo consortium

The three Committees will be informed of any significant modification to the Protocol and the appearance of any serious and unexpected changes occurring during the project susceptible of affecting the safety of users or the conduct of the research.

1.6 Ethics Code for Professionals

The Ethics Code for Professionals is foreseen in WellCo, to guide the commitment of the professionals involved in this project. The proposed text for the Ethics Code for Professionals is enclosed in the Appendix *Confidentiality and Professional Ethics Agreement*

The ethics code is not only applicable for those beneficiaries which are pilot sites, but the whole consortium. All data gathered by the pilot sites or even directly from the end-users´ interaction with WellCo platform or by the used of the wearable devices foreseen in the project. These data will be processed by all technical partners and not only by the pilot sites**. Data will be anonymized (or at least pseudo-anonymized) as far as possible, without damage for the impact of the project.** Partners can anonymise the identity of participants, including their localtion; however, once the user creates a profile in the WellCo app, it is not possible to anonymise her/his data because it is required to know the relation between subjets and personal data just for providing accurate information and personalised recommendations.

PART II: Gender

As regards the gender perspective, WellCo addresses the Responsible Research & Innovation principles, RRI; so, **moRRI indicators**[1] will be integrated within the project evaluation as a very relevant assessment tool for ethics and gender issues.

Gender equality will be promoted through:

- **Horizontal and vertical participation of women** in research, due to their underrepresentation and lack of involvement in management and decision-making processes.
- **Structural change** in institutions aimed to eliminate barriers and to enhance scientific careers of women and girls.
- **Gender in research content,** as a relevant perspective for analysing and tackling complex topics.

Relevant indicators will be selected for evaluating the project, during its whole lifecycle. Moreover, these long-term outcomes will be considered for designing activities, networking strategy and dissemination and communication plans. In order to accomplish a consistent perspective in research and innovation within the WellCo project, Public Engagement and Science Literacy will be considered within the general ethical framework and, thus, the gender approach. WellCo will contribute to educate and generate awareness through providing reliable and evidence-based information on seniors' health-related issues in an affordable and friendly way aimed at co-creating new knowledge through the collaboration of experts and non-experts

Several topics have been detected as relevant concerning gender equality. It must be noticed that the traditional gender roles have influenced health outcomes and behavioural change of women as well as their use of technology; from the point of view of Social Determinants of Health and social epidemiology, gender is also a relevant dimension that requires a separate evaluation for acknowledging all potentially related issues and reaching a comprehensive evaluation of the project outcomes. These differences should be integrated into the activities design **– in-line with the RRI perspective** – as well as within the evaluation and the project management when applies to the participation of women in the project and, in general, in research or piloting/validation activities.

In addition, intrinsecally related to the gendered perspective, the intercultural and culturally comprehensive design & evaluation methodology will aim to provide evidence-based and consistent solutions for involving older women in an inclusive way, due to their potential reluctance or lower self-confidence to ICT tools.

As regards the gender in the research itself, specific elements will be analysed a) gender behaviours; b) gender factors on ICT use and self-confidence with this regard; c) gender disparities regarding physical activity and self-management of health and disease; d) quality of life and wellbeing; e) the impact of gender roles; f) health-related behavioural change potential and differences in women and men.

Researchers will avoid to use potentially sexist language and discriminatory treatment. In addition, the consortium composition will assure a proportionate ratio of women:men.

[1] Metrics and indicators of. Responsible Research and Innovation. Progress report D3.2. Monitoring the Evolution and Benefits of. Responsible Research and Innovation (MoRRI) https://www.rri-tools.eu/documents/10184/47609/MORRI-D3.2/aa871252-6b2c-42ae-a8d8-a8c442d1d557

All these measures are detailed in the following sub-sections, so the following principles[2] will be taken into account in the whole process to build WellCo: design, development, testing and assessment.

2.1. Social determinants of health (SDH)

Traditional gender roles and naturalised behaviours conditions behaviours and expectancies of women and men; it directly implies different responsibilities within the society (public) and the family (private). Their gender and the social construct behind determine, for example, a different exposure to risky conditions and, also, the whole research agenda in Public Health or the health communication inside and outside the system and its institutions[3]. Traditional gender roles are also related to the engagement, involvement, interests and self-management abilities. In-line to the RRI principles stated above, these differences should be further studied in order to evaluate the project performance and its long-term impact at societal level. Leadership of women within the virtual community will be also encouraged [4]

In addition, the vast majority (81%) of full-time informal caregivers are women [5]. Caregivers with no formal competence perceived higher workload, more communication obstacles, less competence, poorer sleep and more stress symptoms than did their colleagues (formal caregivers)[6]. Women aged over 65 with lower educational attainment have shown increased risk of worsening in frailty state (weakness, weight loss, exhaustion, slowness and low activity). Women's greater longevity means that they are more likely than men to live with disability; disabilities condition unique and gender-specific health concerns related to their roles in society. Cultural and social issues can impact on women's health and are important to consider in health services planning and research[7]; in addition, their disempowerment – in a broad sense – undermine their relations with healthcare professionals and researchers, excluding older women from participating in testing and innovative health solutions.

- **Health disparities** and social consequences of ageing are different for women and men[8]. Research shows an increased risk of low income for older women, that means, for example, they are more likely to live in unsafe places, isolation and have less possibilities for adapting their homes to improve its accessibility [9]

2 WHO Regional Office for Europe: "Women's health and well-being in Europe: beyond the mortality advantage". ISBN 978 92 890 5191 0

[3] Verbakel, Ellen, Stian Tamlagsrønning, Lizzy Winstone, Erlend L. Fjær, and Terje A. Eikemo (2017) Informal Care in Europe: Findings from the European Social Survey (2014) Special Module on the Social Determinants of Health. European Journal of Public Health 27(suppl_1): 90–95. https://academic.oup.com/eurpub/article/3045950/Informal, accessed September 11, 2017.

[4] Folta, S. C., Seguin, R. A., Ackerman, J., & Nelson, M. E. (2012). A qualitative study of leadership characteristics among women who catalyze positive community change. BMC Public Health, 12(1), 383. https://doi.org/10.1186/1471-2458-12-383

[5] Jang, Soong-Nang, Mauricio Avendano, and Ichiro Kawachi (2012) Informal Caregiving Patterns in Korea and European Countries: A Cross-National Comparison. Asian Nursing Research 6(1): 19–26. http://linkinghub.elsevier.com/retrieve/pii/S1976131712000035, accessed August 25, 2017.

[6] ENGSTRÖM, M., SKYTT, B., NILSSON, A., Vårdvetenskap, vårdvetenskap, A. för hälso-och, Gävle, H. i, & arbetsliv, A. för hälsa och. (2011). Working life and stress symptoms among caregivers in elderly care with formal and no formal competence. Journal of Nursing Management, 19(6), 732–741. https://doi.org/10.1111/j.1365-2834.2011.01270.x

[7] Jacobson, N., Trojanowski, L., & Dewa, C. S. (2012). What do peer support workers do? A job description. BMC Health Services Research, 12(1), 205. https://doi.org/10.1186/1472-6963-12-205

[8] Kim, J. I., & Kim, G. (2017). Socio-ecological perspective of older age life expectancy: Income, gender inequality, and financial crisis in europe. Globalization and Health, 13 doi:10.1186/s12992-017-0279-8

[9] Michalos, A. C. (2017). Connecting the quality of life theory to health, well-being and education : The selected works of alex C. michalos. Cham: Springer.

- Life **expectancy** across Europe differs by up to 15 years for women, so females are more exposed and vulnerable to chronic illnesses and serious mental disorders at the same time that they have a lower socio-economic position. Loneliness is also a psychological health issue related to deleterious physical health outcomes such as mortality and chronic disease[10]
- Cardiovascular diseases continue to comprise a major part of the overall disease burden for women, but rates of mental ill health are increasing throughout the EU and across all ages[11].[12]

2.2. Inequality

- **Gender inequalities produce health disparities**. These inequalities, discrimination and gender stereotypes are important underlying factors influencing behaviour and practices that affect health across their life-course. WellCo is designed to promote gender equity in the promoting healthy ageing, particularly among those who are elderly carers (formal and informal) of elderly relatives.

2.3. Life-course approach

- WellCo addresses social determinants of health, so, among others, culture, gender and socioeconomic/sociocultural position, as well as evidence on biology, comprehensively merged for clarifying how the ageing process determines well-being and quality of life from a multidisciplinary point of view. Moreover, WellCo aims at clarifying how these dimensions could be approached from a specific gendered framework as regards women and men during their whole lives.

2.4. Balanced participation

- The balance will be ensured through engaging women and men as participants for co-designing the platform. Specific efforts based on an evidence-based theoretical framework will be devoted to reaching a balanced sample as regards sexes and genders involved. Furthermore, a gender balance in the professional team involved in the Project will be addressed.

2.5. Questions orientation

- As explained above, gender-related variables are important for describing how being a woman or man conditions behaviours, experiences, expectancies and health outcomes. Questions included in questionnaires, surveys and any other activity related will be gendered and will ask for specific information to women and men. These will be also inclusively written.

[10] Curran, T. (2018). Intergenerational Transmissions of Mother-Child Loneliness: A Moderated Mediation Model of Familial Social Support and Conflict Avoidance. Health Communication, 0(0), 1–7. https://doi.org/10.1080/10410236.2018.1466229

[11] Kessler, R. C., Aguilar-Gaxiola, S., Alonso, J., Chatterji, S., Lee, S., Ormel, J., … Wang, P. S. (2009). The global burden of mental disorders: An update from the WHO World Mental Health (WMH) Surveys. Epidemiologia E Psichiatria Sociale, 18(1), 23–33.

[12] Vos, T., Barber, R. M., Bell, B., Bertozzi-Villa, A., Biryukov, S., . . . Avdelningen för psykologi. (2015). Global, regional, and national incidence, prevalence, and years lived with disability for 301 acute and chronic diseases and injuries in 188 countries, 1990–2013: A systematic analysis for the global burden of disease study 2013. Lancet, the, 386(9995), 743-800. doi:10.1016/S0140-6736(15)60692-4

2.6. Gender-responsiveness

- The "Life Plan" will be very useful to take into consideration the main gender differences to adapt WellCo to the likes, desires and life expectations with a gender approach. It can be used as a tool to ensure a **gender responsive solution.**

2.7. Recruitment

- Women in Europe comprise most of the older population, with the proportion being even higher for those aged 80 and older[13]. Consequently, an effort will be made in the recruitment process to try to balance the women:men participation ratios in a proportionate way as regards the reference population.
- While there is a lack of evidence on older women enrolment and engagement in ICT-mediated health and mHealth[14][15], the calculation of the sample within the WellCo project will also aim at overcoming the existent barriers in recruitment of seniors reaching a balanced sample in this sense,i.e., reproducing the socio-demographic characteristics of each cultural background and contextual environment.

2.8. Design

- The design for Mock up will pay attention to gender, as part of the Socio-Economic Status patterns that could influence the personalization of recommendations – the three incremental prototypes will bear in mind to fulfil gender expectations.

2.9. Motivation

- Virtual recommendations will be based on different motivating activities, gender approached, trying to design a co-participation process that may involve all gendered behaviours and will be adapted to the specific age group.
- In sum, virtual recommendations will be culturally comprehensive from a gender point of view – but not restricted to gender – all will tend to transmit and share the specific subcultures for older women and men for merging both to enrich the participation and the outcomes of persons involved.

2.10. Recommendations

- All these aspects underlined above will be taken into consideration when offering recommendations.
- Also, the last evidence on research of wellbeing and healthy lifestyles will consider gender as a key aspect: the health system providing care based on a male standard, for example, may not appropriately address gendered-analysed health needs and disparities.

13 Rodrigues R, Huber M, Lamura G, editors. Facts and figures on healthy ageing and long-term care. Vienna: European Centre for Social Welfare and Research; 2012 (http://www.euro.centre.org/detail.php?xml_id=2079, accessed 20 July 2016)

[14] Vroman, K. G., Arthanat, S., & Lysack, C. (2015). "Who over 65 is online?" Older adults' dispositions toward information communication technology. *Computers in Human Behavior*, *43*, 156-166.

[15] Göransson, C., Eriksson, I., Ziegert, K., Wengström, Y., Langius-Eklöf, A., Brovall, M., ... & Blomberg, K. (2017). Testing an app for reporting health concerns—Experiences from older people and home care nurses. *International journal of older people nursing*.

2.11. Dissemination

- A special consideration will be made for dissemination actions. A leaflet with information related to the project with plain language address to older citizens will be edited, including gendered pictures and messages – so, inclusive and reflecting images of women and men from different cultural background and contextual settings - for engaging potentially reluctant seniors meanwhile transmitting a positive image of older persons to the whole society.

PART III: Data Protection[16]

3.1. Disclaimer

Only the data protection aspects concerning data gathering are included in this document. Those questions related to the protection of data after its gathering (storage, processing, transfer and sharing) will be subject to the deliverable "D6.6 Open Data Management Plan", as part of WP6.

3.2. European Regulation on Data Protection

The following section presents the main considerations and provides an overview of key elements on data protection. The application of these considerations to WellCo project is discussed in section 3.4. Data protection Protocol WellCo.

3.2.1. Regulation / Legislation

The processing of personal data is governed since 1995 by the Directive 95/46/EC without direct applicability in the national legislation. The Directive seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

Member states have implemented the Directive on data protection in several national laws and decrees.

In 2016 the European parliament approved Regulation (EU) 2016/679, 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 – GDPR). This new regulation was published on 4th May in the Official Journal of the European Union.

The GDPR shall enter into force on two years after its publication in the Official Journal of the European Union, i.e. 25 May 2018, and shall be binding in its entirety and directly applicable in all Member States.

In addition to the main regulations there are various sectoral legislation texts:

- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 in the protection of individuals regarding the processing of personal data by the Community institutions and bodies and on the free movement of such data.
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA.
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services; in particular, electronic commerce in the Internal Market (Directive on electronic commerce)
- Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
- Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work.

[16] **Disclaimer**. Only the data protection aspects concerning data gathering are included in this document. Those questions related to the protection of data after its gathering (storage, processing, transfer and sharing) will be subject to the deliverable "Open Data Management Plan", as part of WP6.

- Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters.
- Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

3.2.2. Principles / Applicability / Exemptions /Scope

3.2.2.1. Accountability under GDPR

The Data Controller is **responsible** for and should be able to **demonstrate compliance** with the GDPR. Any action taken in order to achieve compliance with the mentioned principles should be **duly documented** to be able to provide such documentation to the competent authorities when needed.

3.2.2.2. Lawfulness, fairness and transparency under GDPR

- **Lawfulness:** anytime personal data is processed, the processing must be lawful, meaning that it should be based on at least one recognized legal ground.
- **Fairness & transparency:** the data subject must be informed of the existence of the processing operation, its purposes and the potential consequences.

The legal grounds for the processing of **personal data** are:

- Consent[17]
- Performance of a contract
- Legal obligation
- Vital interest
- Public interest
- Balance of legitimate interests
- There are some specific legal grounds for processing **sensitive data** and **criminal data.**

Legal grounds for the processing of **sensitive data:**

- Explicit consent[18]
- Legal obligation
- Vital interest
- Non-Profit
- Public data
- Legal claims
- Public interests
- Public health
- Research[19]

Legal grounds for the processing of **criminal data:**

- Under the control of an official authority
- Expressly authorised by law

17 Necessary for processing some data in the present project WellCo

18 Necessary for processing any sensitive data in the present project WellCo

19 Depends on any project to get the recognition of "research"

3.2.2.3. *Purpose Limitation*

Personal data may only be collected and processed for achieving **specific purposes.**

These purposes must be **legitimate,** and the purpose must be **clearly specified to the data subjects** from the start (for example in a Privacy Policy or Statement).

Any further processing must be compatible with the initially specified purposes and communicated to the data subject (**compatibility).**

3.2.2.4. *Data minimisation*

Personal data which are collected and otherwise processed should be **adequate, relevant** and **limited to what is necessary** in relation to the purposes.

Concerning this issue, it is interesting to point out that some companies or other entities may be tempted to collect "as much data as possible", thinking that these data may serve someday. However, minimising the amount of collected data is positive in many aspects: it may facilitate storage, monitoring and updating and cleaning operations, and may also help mitigating or minimising other risks such as data leaks or other data breach incidents.

3.2.2.5. *Accuracy*

Personal data should be **accurate** and, when necessary, **kept up to date.**

- Every reasonable step should be taken to ensure that inaccurate or outdated data are **erased, updated or rectified** without unnecessary delay or at the instance of the data subject.
- **Verification and correction mechanisms** should be put into place, whereby data subjects can easily notify any error/mistake.

3.2.2.6. *Storage limitation*

Personal data should be kept for no longer than necessary for achieving the legitimate purposes of the processing. Once the purposes are achieved, it is required to either erase the data or to anonymise them.

The **only exception is an archiving purpose** in the public interest, or for statistical, scientific or historical research purposes.

3.2.2.7. *Integrity and confidentiality*

Personal data should be at all times processed in a manner that ensures both:

- **Integrity**: measures to protect the data against unauthorised or accidental loss, destruction or alteration
- **Confidentiality**: measures to protect the data against unauthorised; or accidental use or disclosure).

3.2.2.8. *Working Party Article 29 Directive 95/46/EC (Data Protection Directive), of 24 October 1995 "Group of the Protection of Individuals when Processing Personal Data"*

WP29 is an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. The tasks of WP29 are set out in Article 30 Directive 95/46/EC and Article 15 2002/58/EC. Thereafter, the group has primarily advisory function. It may also make recommendations and opinions on any matter concerning the protection of individuals with regard to the processing of personal data in EU. The audit standard is in particular the two mentioned privacy policies.

The comments and guidelines of the group are not binding. The WP 29 is independent of the EU institutions and bodies and makes its decisions according to the majority principle.

General Remark on WP29 recommendations on the GDPR application

From 25 May 2018, the date of application of the GDPR, the WP29 will be replaced by its de facto successor, the European Data Protection Committee established under Article 68 GDPR. Due to the different composition of members, it is not certain that the Data Protection Committee adopts the statements, guidelines and opinions of its legal predecessor. Also it is not certain if the working papers of WP29, which already relate to the content of GDPR (and had been considered for the elaboration of the current report), will be made into binding "guidelines", "resolutions" or "recommendations" of the Data Protection Committee, for the creation of which the Data Protection Committee is mandated under Art. 70 GDPR.

However, at the time this report, when there is no development of GDPR, the recommendations made by WP29 should always be taken into account, as so far, the European Committee for Data Protection has not been established.

3.2.3. Definitions / Obligations / Requirements

3.2.3.1. Controller and processor

The controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

The controller has effective control over the data. It determines the purposes (why) and the essential elements of the means (how) of the processing (which data to collect, for what purposes, which software tools to use, etc.). **The controller is nominated as part of the Data Protection Impact Assessment (referred as Data Controller), further detail in section 3.4-** Data Protection Protocol WellCo

3.2.3.1.1. Types of controllers:

Joint controllers: joint controllers are "jointly" (together or not alone) in control of the same personal data.

That means that, with respect to a certain processing activity, different parties determine together either the purpose or the essential elements of the means.

The participation of the parties to the joint determination may take different forms and do not need to be equally shared.

- Art. 26 GDPR: Joint controllers shall, in a transparent manner, determine their respective responsibilities (arrangement).
- Art. 82 GDPR: Joint liability (exemption if not in any way responsible, regress possible)
    - Separate controllers: separate controllers are in control of the same personal data but determine the purposes and means of the processing separately. Each entity determines its processing activities for its own purposes and with its own means, independently from the other entity.
    - The processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The controller instructs the processor. The processor may have some room of manoeuvre in following the instructions but will never be allowed to use the data for other purposes. He/she will always process the data on behalf of and following the instructions of the controller.

Persons working under the direct authority of the controller (e.g. employees or agent) are excluded from the definition of processors. They are considered as the "flesh and bones" of the controller.

The facts always prevail over any private agreement.

Distinction must, in each single case, be determined based on the factual role of the parties, the specific activities of each entity and the specific context in which the data processing activities take place (hybrid relationships are possible).

3.2.3.2. Relationship between the controller and the processor

In case of doubt, the following questions should be asked:

- Who takes the decision up-front to initiate the processing?
- Who decides about the essential elements of processing (e.g. types of data that are collected, for how long, for what purposes, etc.)?

The GDPR strictly regulates the relationship between a controller and a processor. Whenever a controller engages a processor, a written agreement containing certain mandatory provisions must be signed (Appendix - **Contract: Data Controller and Data Processor**).

3.2.3.3. Data processing agreements and data transfer

When personal data are transferred to a third party, there are three relevant questions:

- How does the receiving party qualify?
  - Is it a data controller?
  - Is it a data processor?
- Is there a legal basis for the transfer?
- Where is the receiving party located?

Data processing agreements

- Format.
- Obligation of both the controller and the processor.
- Which template to use?
- Mandatory elements of a processing contract under GDPR:
  - Short description of processing (duration, nature, purpose, etc.)
  - Specification of the type of personal data and the categories of data subjects.

Obligations for the data processor:

1. Processes only on documented instructions from the data controller.
2. Obligation of confidentiality for personnel.
3. Safety measures.
4. Shall not engage another processor without consent of the controller.
5. Assists in responding to requests by data subjects.
6. Assists in ensuring compliance with other obligations in the GDPR.
7. Deletes or returns all the personal data after the end of the processing.
8. Makes available all information necessary to demonstrate compliance with the obligations and allows for audits and inspections.

3.2.3.4. Main obligations for the data controller:

- The controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation.
- Review and update measures if necessary.
- Adherence to approved codes of conduct or approved certification mechanisms to demonstrate compliance with the obligations of the controller.
- When the type of processing (in particular processing using new technologies) may result in a high risk to the rights and freedoms of natural persons, the controller shall,

prior to the processing, carry out an impact assessment (a single assessment may address a set of similar processing operations that present similar high risks).

- If data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk shall consult the supervisory authority prior to processing.
- If necessary, a data protection officer (DPO) will be appointed if
  - Processing is carried out by a public authority or body
  - Core activities consist of processing operation on a large scale
- Records of processing activities:
  - Name and contact details of controller and other intervenient.
  - Purposes of the processing.
  - Description of the categories of data subject and categories of personal data.
  - Categories of recipients of personal data, including third countries or international organisations.
  - Transfer of personal data.
  - If possible, envisaged time limits for erasure of the different categories of data.
  - If possible, a general description of the technical and organisational security measures referred to article 32.

3.2.4. Rights

- Right to rectification.
- Right to erasure ("right to be forgotten").
- Right to restriction of processing.
- Notification obligation regarding rectification or erasure of personal data or restriction of processing.
- Right to data portability.
- Right to object to automated decision-making.
- Right to object.

3.2.5. Data Protection Impact Assessment (DPIA)

3.2.5.1. Data Protection Impact Assessment (Art. 35 GDPR)

3.2.5.2. What is a Data Protection Impact Assessment ("DPIA")?

An assessment that the **data controller** must carry out when its processing activities entail a **"high risk"** for the rights and freedoms of data subjects. Basically, the purposes of conducting a DPIA are: (i) to clearly **identify the existing risks** of the processing activity for the data subjects and (ii) to **find solutions / measures** to be implemented in order to mitigate those risks.

3.2.5.2.1. In case of the WellCo project should a DPIA be conducted?

The European regulation states: *Where your **data processing activities** are **"likely to result in a high risk to the rights and freedoms of a data subject"**,* in particular when using **new technologies**, such as facial recognition, behavioural analysis software, high-tech cameras or other new intelligent software or devices[20].

The term "likely to result in a high risk" includes, a systematic and extensive evaluation of personal aspects relating to natural persons which is based on **automated processing,**

20 In fact, since most of the "live data" about the health of the participants will be obtained by wearables, we should consider if the WellCo project is obligated to conduct a DPIA.

including profiling, and on which decisions are based that produce legal effects concerning the natural person; processing on large scale of **special categories of data** and systematic **monitoring** of a publicly accessible area **on a large scale.**

According to the WP29, the following criteria should be considered (with two of them or less, the DPIA will not be required):

- Evaluation or scoring (including profiling and predicting).
- Automated decision-making with legal o similar significant effect.
- Systematic monitoring.
- Sensitive data.
- Data processed on a large scale.
- Matched or combined datasets.
- Data concerning vulnerable data subjects.
- Innovative use or applying technological or organisational solutions.
- Data transfer outside the EU.
- Processing preventing data subjects from exercising a right or using a service or a contract.

The previous list could be completed by national Supervisory Authorities, as they could establish a **white list** of processing operations which do not imply a high risk.

At the time of elaborating the present report no list exists, then attention must be paid to the pre-established list provided by WP29, and in conclusion, the WellCo project will be processing personal data for profiling[21] and systematic monitoring of the participants applying technological solutions.

The WP29 considers some exceptions: when it has been determined that the processing operations of the company/project entail a "high risk", it is relevant to check whether one of the following two exceptions could apply (it is not the case of WellCo):

- The white list exception
- The public task exception, if general DPIA has already been conducted because the "high risk" processing operations are:
  - Based on a legal obligation (like tax declaration e.g.) or
  - Carried out in the public interest or in the exercise of an official task vested (e.g. prevention of terrorism, police cooperation)

Therefore, no DPIA is necessary unless the national Supervisory Authority specifically requires a second DPIA to be conducted by the company/project.

Where a DPIA is required, it should be carried out **prior to the processing,** but a single DPIA could be used to assess **multiple processing operations.** According to WP29 in cases where it is not clear whether a DPIA is required, a DPIA should be carried out nonetheless, as it is a useful tool to help data controllers comply with data protection law.

3.2.5.2.2. Content of the DPIA

At first, the controller is responsible to carry out the DPIA, and should be assisted by a processor, and if appropriate, the controller must also seek the advice of Data Protection

21 Profiling means any form of automated processing (without human intervention) of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Officer (DPO), as well where appropriate, the controller must seek the views of data subjects or their representatives on the intended processing.

A DPIA should contain:

- A systematic **description** of the envisaged processing operations and the purposes (including, where applicable, the legitimate interests pursued by the controller).
- An assessment of the **necessity and proportionality** of the processing in relation to the purposes.
- An assessment of the **risks** for individuals.
- The **measures** in place to address the risks, including safeguards, security measures and mechanisms to demonstrate compliance.

3.2.6. Transfer of personal data, data confidentiality and security

3.2.6.1. Transfers of personal data to third countries or international organisations

"Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for inward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.
All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by the Regulation is not undetermined."

Article 44.

3.2.6.2. Security

- The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:
  - Pseudonymisation and encryption of personal data – data will be pseudonomised as long as it does not affect the impact of the project, i.e. the accuracy to provide personalized recommendations;
  - Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. In WellCo, access to the database will be performed after a process of authentication/authorization so access will be ensured only for allowed people;
  - Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident – periodic backups will be performed in WellCo;
  - A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- Measures to protect storage of personal data. Hi-Iberia, the coordinator of the project, is compliant with ISO 27000.

3.3. National Regulation on Data Protection[22].

3.3.1. General Considerations

The national regulation will apply to all data processing initiated prior to 25 May 2018, when Regulation (EU) 679/2016, of 27 April 2016, GDPR enters into force. Nevertheless, all data processing must be adapted to GDPR as soon as possible, because the new regulation established more and detailed right for the data subject.

3.3.2. Denmark

3.3.2.1. Regulation

The processing of personal data is governed by the Act on Processing of Personal Data (Lov om behandling af personoplysninger (APPD) implementing Directive 95/46/EC on data protection.

Other acts governing data protection take precedence over the APPD if they offer a better protection for the data subject.

Besides the main regulation there are various sectoral laws:

- Act on the Use of Health Information in the Labour Market (Lov om brug af helbredsoplysninger mv. på arbejdsmarkedet).
- Act of Prohibition against Discrimination in the Labour Market (Forskelsbehandlingsloven).
- Financial Businesses Act (Lov om finansiel virksomhed) governing inter alia disclosure of customer data in financial businesses.
- Health Act (Sundhedsloven) governing inter alia processing and disclosing patient data for purposes of treatment and other purposes within the health sector.
- Executive Order on Cookies (Bekendtgørelse om krav til information og samtykke fra brugeren ved lagring af eller adgang til allerede lagrede oplysninger i slutbrugers terminaludstyr).
- Executive Order on Telecommunications (Bekendtgørelse om udbud af elektroniske kommunikationsnet og –tjenester - Udbudsbekendtgørelsen) governing use and disclosure of traffic data and location data for suppliers of telecommunication nets and services.

3.3.2.2. Applicability / Definitions / Prohibitions

The Danish law applies to:

- Controllers of personal data
- Data processors (in terms of security requirements and certain requirements for authorization from the Danish Data Protection Agency).

A data controller determines the purpose and means of processing personal data whereas a data processor processes personal data on behalf of a data controller.

The APPD does not apply to personal data processed by an individual for purely private purposes (Exemption).

APPD governs personal data, which is defined as any information relating to an identified or identifiable natural person, including encrypted or pseudonymized data. It also contains special provisions governing, for example:

- Credit information and blacklists (both relating to individuals and companies).
- TV surveillance data.

[22] The specific compliance in the WellCo project is furtherly explained in: Data Protection Protocol WellCo

- Registration of telephone numbers.

APPD applies to processing wholly or partly by automatic means and to processing other than by automatic means of personal data, which form part of a filing system.

Parts of the APPD also apply to the private sector's non-automatic systematic processing of private or financial matters or other data on personal matters which may reasonably be demanded to be withheld from the public. This is a Danish provision and does not derive from the Data Protection Directive.

The act includes:

- Collecting
- Integrating
- Storing
- Searching
- Monitoring
- Transferring
- Deleting

The Act on Processing of Personal Data (APPD) applies to data controllers established in Denmark if the activities are carried out within the EU or the EEA, but it also applies to a data controller established outside of the EU in case:

- Processing of personal data is carried out with the use of equipment situated in Denmark (unless the equipment is used purely for the purposes of transmitting personal data through the EU/EEA).
- Collection of personal data in Denmark takes place with the aim to process the personal data outside the EU/EEA (this is a Danish provision and does not derive from the Data Protection Directive).

Also, the APPD applies to the data processing of personal data on behalf of Danish diplomatic representations.

The main rule under the APPD is that personal data can only be processed if one or more of the following conditions are met:

- The explicit consent of the data subject has been obtained (Consent must be explicit and not merely unambiguous).
- For the performance of a contract in which the data subject is a party, or to take steps at the request of the data subject before entering into a contract.
- Compliance with a legal obligation to which the data controller is subject.
- Protecting the vital interests of the data subject.
- The performance of a task carried out in the public interest.
- The performance of a task carried out in the exercise of official authority vested in the data controller or in a third party to whom the data is disclosed.
- The purposes of the legitimate interests pursued by the data controller or by the third party to whom the data is disclosed, and these interests are not overridden by the interests of the data subject.

The conditions vary for personal data, which is sensitive or purely private in nature (purely private data is an extra category of personal data in Denmark).

The main instances where private sector entities must obtain prior authorization from Danish Data Protection Agency include (but are not limited to) the following:

- Processing relating to sensitive personal data about employees, such as:

- Personal testing;
- Logical testing; or
- Information regarding the summary dismissal of an employee.

- Whistle-blower schemes.
- Payment card blacklists.
- Processing relating to sensitive personal data concerning customers, suppliers or other business relations (although there are certain exceptions, for example, for attorney-client relationships).
- Market surveys that involve the processing of sensitive personal data.
- Alternative healthcare providers.

3.3.2.3. Obligations / Consent / Legal grounds

The main obligations for the data controllers are:

- Adherence to "good data protection practices"
- Ensuring that the personal data is collected for specified, explicit and legitimate purposes, and that further processing is compatible with:
  - These purposes, and
  - The purposes for which the personal data was subsequently processed.
- Ensuring that personal data is adequate, relevant and not excessive for:
  - The purposes for which the data was collected; and
  - The purposes for which it was subsequently processed.
- Organizing the processing of data to ensure that the personal data is updated appropriately.
- Deleting or rectifying inaccurate or misleading personal data without delay.
- Not to keep collected personal data in a form which makes it possible to identify the data subject for a longer period than necessary for the purposes for which the data is processed.

Consent is one of the legal grounds for processing of personal data, that must be freely given specific and informed indication of the wishes of the data subject, by which he or she agrees to the processing of his/her personal data.

The consent must be:

- Voluntary and provided verbally or written
- Specific to a particular processing by a particular data controller for a particular purpose.
- Informed, and the data subject must receive all relevant information necessary to assess how the personal data will be processed and be aware that consent has been provided.

The consent either can be obtained online through:

- Opt-in mechanism (ticking a checkbox, opt out mechanism is not valid)
- Opt-in action (using a website after being informed with a notification stating that consent will be implied by using the website)

Implied or inferred consent is insufficient.

In Denmark, a minor is under 18 years of age. Nevertheless, under the Danish Data Protection Agency, consent from minors, as young as 15 years old has been accepted. However, whether a minor can validly consent to the processing of their personal data is assessed on a case by-case basis.

Depending on the type of personal data, there are some other legal grounds to justify processing data.

Non-sensitive personal data:

- Performance of a contract in which the data subject is a party or to take steps at the request of the data subject before entering into a contract.
- Complying with a legal obligation, which the data controller is subject to.
- Protecting the vital interests of the data subject.
- The performance of a task carried out in the public interest.
- Performance of a task carried out in the exercise of official authority vested in the data controller or in a third party to whom the data is disclosed.
- Purposes of the legitimate interests pursued by the data controller or by the third party to whom the data is disclosed, if these interests are not overridden by the interests of the data subject.

In relation to consumers and marketing, there are some specialties; a company must not disclose personal data relating to a consumer to another company for marketing purposes or use such data on behalf of another company for marketing purposes without obtaining consent.

An exception applies if the data relates only to general categories of personal data that are used to divide the data subjects into categories (for example, if a consumer is interested in cars or children's clothes).

Sensitive personal data must not be processed under this provision. The provision is a special Danish provision and does not derive from the Data Protection Directive.

A company must always check on the Danish Civil Protection Registration System to see whether a consumer has generally opted out of marketing activities.

If they have not, the company must provide a two-week opt-out option before using or disclosing the personal data for third party marketing purposes.

Sensitive personal data (APPD provides special rules for sensitive personal data and data of a purely private nature, including personal identity numbers and criminal records):

- Sensitive personal data is data revealing:
  - Race or ethnic origin.
  - Political opinions.
  - Religious or philosophical beliefs.
  - Membership of a trade union.
  - Health.
  - Sex life.

Generally, the processing of sensitive personal data is prohibited, with the following exemptions:

- Explicit consent.
- The processing is necessary to protect the vital interests of the data subject or of another person where the person concerned is physically or legally incapable of consenting.
- The processing relates to data that has been made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The Danish Data Protection Agency has provided authorization for processing the data for certain research purposes.

- The following acts contain stricter provisions than the APPD, particularly in the context of employment relationships:
    - Act on the Use of Health Information in the Labour Market.
    - Act on Prohibition against Discrimination in the Labour Market.

Other sensitive personal data:

The APPD contains a provision on criminal offences, serious social problems (for example, the results of personality tests or summary dismissal).

The processing of this sensitive data is also generally prohibited, with the following exemptions:

- One of the general exemptions applies.
- Revealing the data is in the public or private interest (including the best interests of the data subject) and clearly overrides the interests of confidentiality of the data subject.

In relation to the personal identification numbers assigned to each resident (CPR-number) used for interactions with public authorities, healthcare providers and financial institutions, the ADDP establishes that private sector entities can process personal identification numbers if:

- Provided by a law or regulation.
- The data subject has given explicit consent.
- The processing is carried out solely for scientific or statistical purposes.

Identification numbers can be disclosed if:

- Occurring as part of the ordinary operations of a company, and the disclosure is important for identifying an unambiguous individual.
- Requested by a public authority.

Any company must obtain the explicit consent of the individual to publicize a personal identification number.

3.3.2.4. Rights

Rights of individuals:

Collection from an individual.

The data controller must provide certain information to data subjects when collecting personal data:

- Identity of the data controller and any representative.
- The purpose of the data processing.
- Any further information necessary to enable the data subject to safeguard his interests, having regard to the specific circumstances, such as:
    - The categories of recipients;
    - Whether replies to the questions are obligatory or voluntary, as well as possible consequences of failure to reply; and
    - The right of access to data relating to the data subject and the right of rectify it.

Data not collected from an individual.

If the personal data is not obtained directly from the data subject or where disclosure to a third party is envisaged (the latter is not derived from the Data Protection Directive), the data controller must, at the time of the collection of the personal data, provide the individual with the following information:

- The identity of the data controller and any representative.
- The purposes of the processing of the personal data.
- Any further information which is necessary, having regard to the specific circumstances in which the data is obtained, to enable the data subject to safeguard these interests, such as:
  - The categories of data concerned;
  - The categories of recipients;
  - The right to access and rectify the data relating to the data subject.

Exemptions:

Notification requirements do not apply if the data subject has already received the information or if the data subject's interest in obtaining the information is overridden by essential considerations of private interests. The latter is a Danish exemption and not derived from the Data Protection Directive.

Additional, exemptions apply if personal data is not collected from the data subject or where disclosure to a third party is envisaged, for example if:

- Recording or disclosure is expressly set out by law or regulations.
- Providing the personal data to the data subject proves impossible or would involve a disproportionate effort.

In addition to the prior right to receive information:

- Submit a subject access request.
  - Rectify, erase or block misleading or inaccurate personal data.
  - Object.
  - Withdraw consent.
  - File a complaint with the Danish Data Protection Agency.

Right to submit a subject access request

On the request of the data subject, the data controller must provide information about whether personal data relating to the data subject has been processed. If personal data has been processed, the data controller must provide certain information within four weeks. The information must include:

- The data being processed (an overview, not an exact copy of the data).
- The purposes of the processing.
- The categories of recipients of the personal data.
- Any available information regarding the source of the data.

A data subject who has received this information about personal data is not entitled to receive the information again until six months after the latest communication (unless he or she can establish a specific interest in receiving the information in the meantime). A fee of up to DKK200 may be charged if the individual has requested a written answer to the request.

Right of rectification, erasure or blocking of misleading or inaccurate personal data

The controller must rectify data that is inaccurate, misleading or processed in violation of the law in any other way.

On the request of a data subject, the data controller must also notify any third parties to whom the personal data has been disclosed of any rectification of the data (unless such notification proves impossible or involves a disproportionate effort).

Right to object

A data subject can object to the data controller's processing of his/her personal data at any time. If the objection is justified, all further processing must stop.

Third party marketing purposes

A data subject can object to disclosure of personal data to a third party for marketing purposes or use of personal data on behalf of a third party for such purposes.

Before a company discloses personal data to another company for marketing purposes or uses the personal data on behalf of a third party for marketing purposes, it must check in the Danish Civil Procedure Registration System as to whether the consumer has filed a statement that they do not want to be contacted for marketing purposes.

If so, the data controller cannot disclose the personal data or use it for third party marketing purposes. If the consumer has not filed such a statement, the company must give the consumer a two-week notice period to object to the disclosure/use of personal data for third party marketing purposes.

If no objection is received before the end of the two weeks' notice period, the disclosure/processing can take place.

Additionally, the Danish Marketing Practices Act must be adhered to when contacting an individual, especially the prohibition against sending unsolicited email marketing[23].

Automated individual decisions

If the data subject objects, the data controller cannot subject them to a decision based solely on the automated processing of personal data that is intended to evaluate certain personal aspects that will have a legal effect or will significantly affect them.

Exceptions:

- Taken while entering into or performing a contract, if the data subject's request for entering into or performing the contract is satisfied or there are suitable measures to safeguard the data subject's legitimate interests.
- Authorized by a law that also sets out measures to safeguard the data subject's legitimate interests.

23 Under the Danish Marketing Practices Act, advertising using electronic mail or another automatic system is permitted if the individual has given prior consent. If consent has been given, the data subject must be given the opportunity to opt- out in each marketing communication. The opportunity to opt-out must be free of charge and easy to do.

Without consent, an opt-out exception applies if all of the following conditions are met:

The customer has provided their email address or telephone number in connection with a purchase of a product or service.

The customer has been provided with an opt-out option at the time of providing their information.

The customer is provided with an option to opt-out free of charge and in an easy manner in every communication.

The communication is sent by electronic mail (not text messages/SMS).

The company only advertises its own products or services.

The company only advertises similar products or services.

The data subject has a right to be informed by the data controller as soon as possible and without undue delay about the rules on which such a decision is based.

Right to withdraw consent

An individual is entitled to withdraw consent. After withdrawing consent, the data controller is unable to continue processing the personal data.

However, if the data controller can process the personal data under another legal ground, the continued processing can be permitted under the Act on Processing of Personal Data.

Right to request the deletion of data

Data subjects have the right to request the deletion of their data. At the request of the data subject, the data controller must delete or block personal data that is inaccurate or misleading or in any other way processed in violation of the Act on Processing of Personal Data. Therefore, it will depend on a legal assessment whether the request should be complied with.

On the data subject's request, the data controller must also notify any third party to whom the data has been disclosed of any deletion or blocking of the personal data (unless such notification is impossible or involves a disproportionate effort).

3.3.2.5. Security requirements / Communication / Transfer

Security requirements

The APPD contains a general provision obliging the data controller to implement appropriate technical and organizational security measures to protect data from:

- Accidental or unlawful destruction.
- Loss or alteration.
- Unauthorized disclosure abuse.
- Other processing that is in violation of the APPD.

The security requirements vary for public and private entities.

Public entities

The Executive Order on Security Measures for Protection of Personal Data that is processed in the Public Administration provides technical and organizational security that is applicable to public administration. In addition, state entities must adhere to the Information Security Management System Standard ISO 27001.

The Danish Data Protection Agency (DDPA) recommends that private sector entities comply with the Executive Order.

The main obligations under the Executive Order are as follows:

- The data controlling authority must set out detailed internal provisions for the authority's security measures. The provisions must govern organizational issues and physical security, including security organization, administration of access control systems and authorization systems, and authorization control. The internal provisions must be reviewed at least once a year.
- Training and instructions must be provided to employees processing personal data.
- If the personal data is processed by a data processor on behalf of the data controller, the parties must enter into a written contract (Contract: Data Controller and Data Processor**)** stating that the regulations in the Executive Order also apply to processing by the data processor.
- Only individuals with authorization may have access to the personal data that is processed.

- Encryption is necessary when transmitting sensitive personal data or personal identification numbers over the open internet, or e-mails.

Private entities

In addition to the general obligations provided in the APPD, private entities must also fulfil certain conditions relating to security. This is provided in the various permissions granted by the DDPA to process human resources related sensitive data and whistle-blower schemes. These security requirements are like the ones provided under the Executive Order.

Additionally, the DDPA has issued guidance to the effect that transmissions of sensitive personal data and personal identification numbers must be encrypted when taking place over the open internet, but not for e-mails as is the case for the public sector.

Notification of personal data security breaches to data subjects or the national regulator.

Data controllers are not required to notify security breaches to the Danish Data Protection Agency (DDPA).

A data controller may (depending on the circumstances) be required to notify a data subject of a security breach under the general clause on "good data protection practices". For example, the DDPA has held that individuals must be notified without delay of data breaches involving the accidental publication of personal data on the internet.

Processing by third parties

If a data controller delegates the processing of data to a data processor, the data controller must instruct the data processor and ensure that the data processor is able to implement the necessary technical and organizational security measures.

The data controller and data processor must conclude a written contract (See **Contract: Data Controller and Data Processor**) specifying as a minimum:

- The roles of the parties.
- That the data processor can only process data in accordance with the data controller's instructions.
- The applicable data security requirements.
- In addition, the data controller must verify that he data processor carries out the processing in accordance with the instructions during the term of the contract (for example, through audits or review of documentation for the implemented security measures).

Electronic communication (Cookies and equivalent devices on terminal equipment)

Under the Executive Order on Cookies, natural and legal persons cannot store information, gain access to information or let a third-party store or gain access to information, as well as clear, precise and easily understood guidance on how the end-user's informed consent to the storing of, or access to, the information. This information must:

- Appear in a clear, precise and easily understood language or as icons.
- Contain details of the purpose of the storing of, or access to, information in the end-user's terminal equipment.
- Contain details that identify any natural or legal person arranging the storing of, or access to, the information.
- Contain a readily accessible means by which the end-user can refuse consent or withdraw consent to storing of or access to information, as well as clear, precise and easily understood guidance on how the end user can do this.

- Be immediately available to the end-user and be communicated fully and clearly to the end-user. In addition, when storing information or access to information takes place through an information and content service, the information to end-users must be clearly marked and accessible by the end-user on the information and content service in question always.
- The information must be immediately available to the users and easy to access, and the end-user has the right to withdraw an already given consent.

There are two exemptions to the requirement for informed consent. This is when the storing of, or access to information:

- Takes place for the sole purpose of carrying out the transmission of a communication over an electronic communications network.
- Is necessary for the provision of an information society service explicitly requested by the end-user to provide this service.

International transfer of data (transfer outside jurisdiction)

The transfer of personal data within an international group of companies is subject to the same restrictions as the transfer of personal between unrelated third parties.

Denmark is a member state of the EU. Greenland and the Faroe Islands are non-EEA countries.

Transfer within the EU and the EEA

The transfer of personal data to other countries within the EU and EEA is not subject to any additional requirements.

Transfer to non-EEA countries

For transfers to a non-EEA country, additional requirements apply depending on whether the EU Commission has issued an adequacy decision or not for the specific country.

An adequacy decision determines whether or not the relevant country has an adequate level of protection of personal data.

Non-EEA countries with an adequacy decision. The following countries are recognized as generally having an adequate level of protection of personal data:

- Andorra
- Argentina
- Australia (limited to the transfer of air passenger name records).
- Canada (limited to commercial organizations and subject to certain legislation).
- Faroe Islands.
- Guernsey.
- Isle of Man.
- Israel.
- Jersey.
- New Zealand.
- Switzerland.
- Uruguay.
- US (limited to the transfer of air passenger name records).

As a rule, the transfer of sensitive personal data and purely private data to a recipient in any of these countries requires the prior authorization of the Danish Data Protection Agency (DDPA).

Non-EEA countries not having an adequacy decision. The DDPA may authorize a transfer of personal data to a non-EEA country without an adequacy decision if the data controller demonstrates adequate safeguards with respect to the protection of the rights of the data subject by one of the following means:

- EU's Standard Contractual Clauses on transfers of personal data to third countries (SCCs).
- Implementing Binding Corporate Rules (BCR).
- Ad hoc contracts approved by the DDPA.

In addition, personal data can be transferred if the:

- Data subject has given explicit consent to the transfer.
- Transfer is necessary for the performance of a contract between the individual and the data controller or the implementation of pre-contractual measures taken in response to the individual's request.
- Transfer is necessary for the conclusion or performance of a contract, concluded in the interest of the data subject between the data controller and a third party.
- Transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.
- Transfer is necessary in order to protect the vital interests of the data subject.
- Transfer is necessary for the prevention, investigation and prosecution of criminal and the execution of sentences or the protection of persons charged, witnesses or other persons in criminal proceedings.
- Transfer is necessary to safeguard public security, the defence of the realm (which includes Denmark, the Faroe Islands and Greenland) or national security.

Bulk transfers or repetitive transfers cannot take place based on these exceptions but in reliance on SCCs or BCRs.

Data that is processed for public administration and is of special interest to foreign authorities must be stored and processed in Denmark. This is to ensure that the personal data can be disposed of or destroyed in the event of war or similar conditions.

Data controllers can rely on three sets of standard contractual clauses, approved by the EU Commission, covering transfers to another data controller (2001 or 2004 clauses) or to a data processor and sub-processors (2010 clauses).

In addition to the separate grounds for the international transfer, the basic principles and legitimate grounds for the data processing must be complied with for the transfer.

The approval of the Danish Data Protection Agency (DDPA) is not required provided that the data transfer agreement is completely identical to the standard contractual clauses approved by the EU Commission.

If the contractual clauses deviate from the Commission's standard contractual clauses, the exporter must seek to obtain authorization from the DDPA before the transfer. The DDPA does not accept a multi-party setup of the standard contractual clauses.

3.3.2.6. Enforcement and sanctions

The Act on the Processing of Personal Data (APPD) supervises the enforcement powers of the Danish Data Protection Agency. The APPD's powers include (among others):

- Conducting an inspection of recipients of authorizations from the DDPA.
- Issuing a ban or an enforcement notice for breaches of the APPD.
- Demanding rectification, erasure or blocking of specific data.
- Ordering a private data controller to discontinue processing operations.

- Filing reports to the police.

Sanctions and remedies.

The data controller is liable for any damage (including non-financial damage) caused by the processing of data in violation of the Act on Processing of Personal Data (APPD) unless it is established that such damage could not have been averted through the diligence and care required in connection with the processing of data.

Violations of the APPD or a decision or a requirement of the Danish Data Protection Agency is punishable with a criminal fine and potentially up to four months' imprisonment.

Fine levels for non-compliance with the APPD are low, and in practice vary from between DKK3.000 to DKK25.000.

3.3.2.7. Danish Agency of Data Protection

Datatilsynet
Borgergade 28, 5
1300 Copenhagen K
Tel. +45 33 1932 00
Fax +45 33 19 32 18
E-Mail: dt@datatilsynet.dk
Website: http://www.datatilsynet.dk/

- Art 29 WP Member: Ms. Cristina Angela GULISANO, Director, Danish Data Protection Agency (Datatilsynet)
- Art 29 WP Alternate Member: Mr. Peter FOGH KNUDSEN, Head of International Division at the Danish Data Protection Agency (Datatilsynet)

3.3.3. Italy

3.3.3.1. Regulation / Definitions / Scope

Italy has implemented Directive 95/46/EC (prior to the new R(EU) 2016/679) on data protection through Legislative Decree No. 196/2003, the Italian Data Protection Code.

Recently, the Italian parliament passed Law No. 163/2017 (Enabling Law) to prepare for the entry into force of R(RU) 679/2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data (GDPR).

The law enables the government to enact, within six months from the entry into force of the enabling law, one or more legislative decrees to:

- Expressly repeal the provisions of the Data Protection Code that are incompatible with the GDPR.
- Amend the Data Protection Code to the extent necessary to implement the provisions of the GDPR that are not directly applicable, including the current framework for administrative fines and criminal sanctions.
- Resort, if appropriate, to specific implementing and supplemental acts of the Italian Data Protection Authority (IDPA or Garante per la Protezione dei Dati Personali "Garante").

The Enabling Law entered into force on 21 November 2017 and, to date, no legislative decrees have been approved regarding the above matters.

On 28 April 2017, the IDPA published guidelines that, alongside a description of the innovative provisions contained in the European regulation, highlight certain rules of the Data Protection Code that must be considered unchanged.

Over the last months, the IDPA has started publishing documents aimed at identifying which IDPA provisions will remain applicable after 25 May 2018 as well as future measures that the IDPA plans to adopt in the coming months.

In addition to the above, the following provisions should be considered in relation to data protection:

- Article 2 of the Italian Constitution, which recognizes and protects the inviolable rights of individuals, both individually and within the social groups in which they express this personality.
- Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms 1950, ratified by Italy through Law No. 1955 of 4 August 1955, which recognizes the right of individuals to respect for private and family life.
- Strasbourg Convention for the Protection of Individuals regarding Automatic Processing of Personal Data 1981.
- Article 8 of the Charter of Fundamental Rights of the European Union, which recognizes the right to the protection of personal data.
- Directive 2002/58/EC on the protection of privacy in the electronic communications sector.

Beside the main legislation regulating data processing in Italy other laws contain relevant provisions:

- Law No. 633/1941 on copyright protection.
- Law No. 300/1970 (Workers' Statute), right to privacy of employees'
- Legislative Decree No. 70/2003, implementation of Directive 2000/31/EC on certain legal aspects of information society services (electronic commerce)
- Legislative Decree No. 206/2005 (Consumer Code), consumer protection.

In addition, the IPDA has the power to issue binding general provisions on data protection matters (Conduct codes). For example, for processing of biometric data and health data.

Scope of legislation: The Data Protection Code grants rights to data subjects (natural persons) and imposes certain obligations on the following persons:

- Data controller. The data controller is the natural or legal person, public body or other entity who, alone or jointly with others, determines the purposes and means of processing of personal data, including security measures.
- Data processor. The data processor is the natural or legal person, public body or other entity that processes data on behalf of the data controller in the basis of instructions provided by the data controller.
- Person in charge of the data processing. This is the natural person in charge of the data processing on behalf of either the data controller or the data processor. The instrument appointing such a person and the instructions provided must be made in writing.

The definitions of data controller and data processor under GDPR are basically the same as under Directive 95/46/EC which is the base of the Italian Data Protection Code, but the GDPR does not expressly rule out the existence of the person in charge of the data processing, as it refers to "persons authorized to process personal data". Consequently, the rules of the existing Data Protection Code will remain applicable at this point after entering into force or R(EU) 2016/679.

Classification of regulated data.

According to the Italian Data Protection Code, Personal data is defined as any information relating to an identified or identifiable natural person, which means that an identifiable natural person is a person who can be identified, even indirectly, by reference to any other information, including an identification number. The newer GDPR considers technological developments, lice location data and online identifiers.

The national law defines sensitive data as data revealing any of the following:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Membership of religious, political or philosophical associations.
- Health or sexual life.

The above mentioned points are included in the GDPR as "special categories of personal data" complemented by:

- Genetic data.
- Biometric data for the purposes of uniquely identifying a natural person.
- Data concerning a natural person's sexual orientation.

According to the national regulation, data processing occurs whenever any operation or set of operations is performed on personal data, automatically or not, like collection, storage, recording, organization, retrieval, consultation, erasure and dissemination.

3.3.3.2. Applicability / Obligations / Consent

The Italian Data Protection Code applies to the processing of personal data performed by:

- Any entity established in Italy or in a place subject to Italy's sovereignty.
- Any entity established outside the EU that uses for its data processing activities equipment situated in Italy. The only exception of this is equipment used only for purposes of transit through the EU, in the last case the data controller must designate a representative established in Italy with a view to complying with the rules on personal data processing.

The main exemptions are the data processing performed by natural persons for purely personal purposes, with no connection to a commercial or professional activity, as well as other exemptions in relation to certain matters, such as state defence and security matters and data processing performed by some organizations such as public bodies, healthcare professionals and the police).

Data controllers must notify the Italian Data Protection Authority (IDPA) before starting data processing activities if either:

- The data processing concerns certain types of data (such as genetic and biometric data or other data disclosing the geographic location of individuals or objects).
- Personal data is processed for certain purposes (such as profiling purposes or to assess creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful or fraudulent conduct).

Nevertheless, since 2004, the IDPA has published several general provisions setting out exemptions from these notifications, considering that the exempted activities do not prejudice the data subject's rights and freedoms in light of the purposes and means of the data processing.

These exemptions (no applicable to WellCo) are:

- Non-systematic processing activities of genetic and/or biometric data carried out by healthcare professionals, concerning data that is not organized in a database accessible to third parties via electronic networks and to the extent that the processing is necessary for the purposes of safeguarding the data subject's and/or third party's health.
- Processing of personal data disclosing the geographic position of air, sea, and ground transportation channels, where it is only carried out for the purposes of transport security.
- Processing of personal data relating to the data subject's creditworthiness, provided that such data is stored in databases used for certain purposes, such as in connection with the provision of goods or services, or to comply with accounting or tax requirements or regulatory obligations.

Additionally, if the processing of data other than sensitive and judicial data is likely to pose specific risks to data subjects' fundamental rights and freedoms or dignity, the Data Protection Code requires prior checking by the IDPA, which can set specific measures and precautions to safeguard the rights of data subjects.

The GDPR will replace these obligations by conducting data protection impact assessments (DPIA).

Main obligations of the data controller in the Data Protection Code:

- Information notice: to inform the data subject about data processing, the content of information has been expanded by GDPR.
- Principles for data processing:
  - Lawfulness and fairness
  - Purpose limitation
  - Accuracy
  - Proportionality
  - Storage limitation (time not quantity)
- Implementation of security measures: implement minimum and appropriate security measures to ensure data security.

The processing of personal data requires the prior consent of the data subject, that must be given in writing, freely, specifically in relation to a clearly identified data processing, and must be informed.

The Data Protection Code establishes some exemptions of the need of consent if any of the following applies:

- The processing is necessary to comply with an obligation imposed on the data controller by Italian laws and regulations or EU law.
- The processing is necessary to perform obligations stemming from a contract to which the data subject is a party, or to comply with specific requests made by the data subject before entering into a contract.
- The processing concerns data extracted from public registers, lists, documents or records that are publicly available, subject to the restrictions and procedures provided by Italian laws and regulations and EU law in relation to the disclosure and publication of such data.
- The processing is necessary to carry out defence investigations or to establish or defend a legal claim.

- The processing is necessary to protect legitimate interests pursued by a controller or a third party. The Data Protection Code introduced certain restrictions to this legal ground, which were not provided by Directive 95/46/EC on data protection (for example, prior identification by the Italian Data Protection Authority (IDPA) of the cases in which this ground would apply and prohibition against disseminating such data). These additional requirements may be considered inapplicable when the General Data Protection Regulation takes effect.

The processing of sensitive data requires both (Data Protection Code):

- The data subject's written consent.
- Prior authorization from the Italian Data Protection Authority (IDPA).

The IDPA regularly issues general authorizations (typically on an annual basis). These authorizations mainly deal with the processing of sensitive data in specific contexts (for example, in the employment context) or by specific data controllers (for example, lawyers or private investigators).

The latest set of general authorizations was approved by the IDPA in December 2016 and will remain in force until 24 May 2018.

The approach that the IDPA (and the Italian legislator) will adopt in this respect after the entry into force of the General Data Protection Regulation (GDPR) remains unknown, as the GDPR does not expressly require prior authorization for processing sensitive data. However, the GDPR grants EU member states the power to maintain or introduce further requirements, including limitations, about the processing of sensitive data.

3.3.3.3. Rights / Transfer

Section 7 of the Italian Data Protection Code establishes the following data subject rights:

- Right to Access Personal Data.
- Right to be informed of (Section 13):
  - Source of the personal data;
  - Purposes and means/methods of the processing;
  - Logic applied to data processing carried out through electronic means;
  - Identity of the data controller, data processor (if appointed) and established representative in case of trans-border transfers with entities established outside the European Union;
  - Third parties or categories of third parties of whom the data may be communicated (Section 42);
  - Rights he has in relation to the data processing.
- Right to have their data updated, rectified or integrated.
- Right to have their data deleted, anonymized or blocked if processed unlawfully, including data that does not need to be retained in relation to the purposes for which it was originally collected or subsequently processed.
- Right to receive a certification from the entities or individuals to whom the data was communicated that the above processes have been complied with (unless this requirement proves impossible or involves a manifestly disproportionate effort compared to the right that is to be protected).
- The right to object, in whole or in part, to the processing of this personal data:
  - On legitimate grounds;

- Where the processing is carried out for the purpose of sending advertising materials or direct selling for the performance of market or commercial communication surveys.

However, these rights are not absolute in nature and are subject to certain limitations under the Data Protection Code.

Although the General Data Protection Regulation (GDPR) confirms this approach and allows limitations and derogations to the exercise of data subjects' rights, the Italian Data Protection Authority is still analysing whether and to what extent the limitations and derogations set out in the Data Protection Code can be considered compatible with the GDPR.

To exercise the rights mentioned above the data subject has to make a request to the data controller or processor without any formalities and could be made by the agency of a person in charge of the processing. There is no specific period to response but shall be provided without delay (Section 8).

Currently, only providers of publicly available electronic communications services must notify, without undue delay, the Italian Data Protection Authority (IDPA) of personal data breaches (Data Protection Code).

If the breach is likely to be detrimental to the personal data or the privacy of the contracting party or another individual, the provider must also notify that contracting party or other individual without delay.

Over time, the IDPA has extended the applicability of these notification requirements to:

- Data controllers that process biometric data.
- Healthcare professionals, in relation to patients' health data.
- Banks.
- Public entities.

However, when the General Data Protection Regulation takes effect, the requirement to notify personal data breaches will generally apply to all data controllers.

The Data Protection Code allows the transfer of personal data within the EU and the European Economic Area (EEA), and imposes certain limitations on data transfers to third countries (Section 42).

Personal data can be transferred to a third country on any of the following bases:

- Based on the data subject's consent.
- By incorporating standard data protection clauses adopted by the European Commission.
- By using binding corporate rules, if the transfer occurs among companies belonging to the same group but located in different countries.
- On the basis of an adequacy decision of the European Commission.
- For data transfers to the US, under the EU-US Privacy Shield adequacy decision No. 2016/1250 (which replaced the prior EU-US Safe Harbour).

Additionally, personal data can be transferred to third countries when the transfer is necessary to (Data Protection Code):

- Perform obligations stemming from a contract to which the data subject is a party, comply with specific requests made by the data subject before entering into a contract, or execute or perform a contract in the interest of the data subject.
- Safeguard a relevant public interest.

- Carry out defence investigations or establish or defend a legal claim, provided that the personal data is transferred exclusively for these purposes and for the time strictly necessary, in compliance with the laws on business and industrial secrets.

3.3.3.4. IDPA – Italian Data Protection Authority / Sanctions

The Italian Data Protection Authority (IDPA Section 153 - 156) is an independent authority that has the following main enforcement powers:

- Supervise compliance of data processing operations with applicable data protection laws.
- Carry out on-the-spot inspections and access databases, archives, or any other inspection or control at the premises where data processing occurs.
- Order data controllers to adopt necessary or appropriate measures to comply with data protection laws.
- Request data controllers, data processors, data subjects or third parties to provide information and produce documents.
- Prevent, in whole or in part, unlawful or unfair data processing, or block such data processing.
- Report facts that may constitute a criminal offence indictable ex officio by the public prosecutor (of which it becomes aware while performing its duties).
- Impose administrative fines.

Enforcement activities are carried out by the IDPA's staff. When necessary, the IDPA can ask for the co-operation of other state agencies.

A special detail of the Italian regulation of Data Protection is established in Section 12 of the Code, Codes of Conduct and Professional Practice, the national authority (named "Garante" in the Code) shall encourage by having regard to the guidelines set out in Council of Europe recommendations on the processing of personal data.

For this the "Garante" has published a list of codes of conduct in the Official Journal of the Italian Republica that could be consulted by users.

So, the national authority has published different codes of conduct for some specific cases of processing personal data, and to treat the data according to the law, the processors and responsible persons only have to consult these codes of conduct without previous notification to the IDPA (Section 37).

The Data Protection Code provides for administrative fines and/or criminal sanctions in the event of non-compliance with its provisions.

Administrative fines can always be imposed following a finding of criminal liability. However, administrative liability may exist when no criminal offence has been committed.

Additionally, data processing is considered to be a "dangerous activity" subject to Article 2050 of the Italian Civil Code (Article 15, Data Protection Code). This provision reverses the burden of proof and provides that the injured party has the right to be indemnified by the entity that carried out the data processing if that entity is not able to demonstrate that it took all the necessary measures to avoid the damage. The amount of damages awarded is determined by the courts and can include non-pecuniary damages, if applicable.

Administrative fines (Section 142 – 144)

The following main administrative fines apply (Data Protection Code):

- Failure to provide an information notice or providing an inadequate information notice to the data subject: fine ranging from EUR6,000 to EUR36,000.

- Failure to adopt minimum security measures or unlawful data processing: fine ranging from EUR10,000 to EUR120,000.
- Failure to comply with an order of the Italian Data Protection Authority (IDPA) to adopt necessary measures or to block data processing: fine ranging from EUR30,000 to EUR180,000.
- Failure to provide information or documents at the IDPA's request: fine ranging from EUR10,000 to EUR60,000.
- Repeated infringements of certain provisions, when the conduct concerns large databases: fine ranging from EUR50,000 to EUR300,000.

Fines can be doubled if the infringement is particularly serious. Fines can also be increased by up to four times if the original fine may be ineffective in light of the infringer's economic status.

Criminal sanctions

The following main criminal sanctions apply (Data Protection Code):

- Unlawful data processing: imprisonment of up to three years.
- False declarations and notifications to the IDPA: imprisonment of up to three years.
- Failure to adopt minimum security measures: imprisonment of up to two years.
- Failure to comply with an IDPA order: imprisonment of up to two years.

3.3.3.5. Specific Regulation of the Health Sector

Section 75 and 76

3.3.3.6. Garante per la protezione dei dati personali

Piazza di Monte Citorio, 121
00186 Roma
Tel. +39 06 69677 1
Fax +39 06 69677 785
E-Mail: garante@garanteprivacy.it
Website: http://www.garanteprivacy.it/

Art 29 WP Member: Mr. Antonello SORO, President of Garante per la protezione dei dati personali

Art 29 WP Alternate Member: Ms Giuseppe BUSIA, Secretary General of Garante per la protezione dei dati personali.

3.3.4. Spain

3.3.4.1. Legislation

The Data Protection Act (Law 15/1999 on the protection of personal data) implemented Directive 95/46/EC on data protection (Data Protection Directive). It protects individuals with regard to the processing of personal data and the free movement of data. The Regulation developing the Data Protection Act was approved by Royal Decree 1720/2007 of 21 December (Data Protection Regulations).

Besides the main regulation there are no sector-specific laws regulating the processing of personal data, but there are regulations that contain specific provisions on personal data processing (for example, Law 26/2006 on insurance and reinsurance intermediation). The most relevant regulations are:

- Spanish Information Society Services Act (Law 34/2002 on information society services and e-commerce).

- Spanish General Telecommunications Act (Law 9/2014).

In addition, specific legal provisions apply to the processing of:

- Files regulated under the electoral regime legislation.
- Files used exclusively for statistical purposes and protected by legislation on public statistical functions.
- Files for storing data contained in personal classification reports referred to in the armed forces personnel legislation.
- Files derived from the Civil Registry and the Central Registry of Convicts and Fugitives.
- Files from video and audio recordings obtained by law enforcement agencies using video cameras.

3.3.4.2. Applicability / Exemptions / Scope

The Data Protection Act and the Data Protection Regulations apply to data controllers and data processors.

A data controller is any natural or legal person, whether public or private, or administrative body that makes decisions on the purpose, content and use of personal data processing.

Data processors process data on behalf of data controllers as a result of a relationship that links them. A data processor's scope for action is limited by the service it provides to the data controller.

The Data Protection Act and the Data Protection Regulations apply to personal data recorded on physical media for its processing and subsequent use.

Personal data is any information relating to an identified or identifiable natural person (known as the data subject).

Generally, the regulation applies to the processing of personal data:

- Data processing carried out in the context of the activities of an establishment of the data controller in Spain. Where this is not the case, but the data controller uses a data processor established in Spain, the data processor must comply with the provisions on security measures established in the Data Protection Regulations.
- Data processing carried out by data controller not established in Spain but in a place where Spanish law applies by virtue of international public law.
- Data processing carried out by a data controller not established in the European union but using means located in Spain, unless such means are used only for transit purposes. In this case, the data controller must appoint a representative established in Spain.

Data processing means any operation or procedure (whether automated or not) for the collection, recording, storage, elaboration, modification, blocking or erasure of data. It also includes disclosure of data resulting from communications, queries, interconnections or transfers.

Main exemptions where data protection law does not apply:

- Data files maintained by natural persons exclusively for personal or domestic activities.
- Data files subject to the protection of classified matters.
- Data files created to investigate terrorism and serious organized crime.

3.3.4.3. Obligations / Requirements / Registration

Registration of personal data files is required before processing. The data controller must register their data files with the General Data Protection Registry (Agencia Estatal de Proteccion de Datos).

The Data Protection Act and the Data Protection Regulations define data files as sets of structured personal data that can be accessed according to specific criteria, regardless of how the data is generated, stored, organized or accessed. One data file can be composed of several databases (whether automated or non-automated).

Registration is completed through a standard notification from available on the Data Protection Agency's website. Data controllers must complete this form describing, among other aspects:

- The purposes of the data file.
- The categories of personal data it contains.
- Any data disclosures.
- The security level applied to the personal data.
- Any international transfer to third countries.

Registration must be updated whenever there are changes to the data files affecting the information notified to the Data Protection Agency (including removal of the data file).

Main obligations under the Data Protection Act and the Data Protection Regulations. Data controllers must comply with several obligations:

- Complying with the principles of data quality.
- Informing data subjects about data processing on collection.
- Obtaining data subjects' consent to process their data.
- Registering personal data files.
- Implementing security measures to protect personal data, including drafting a security document.
- Attending to data subjects' rights of access, rectification, cancellation and opposition.
- Entering into data processing agreements with data processors.
- Keeping personal data confidential.

Consent from data subjects is required and has to be informed[24]. Depending on the circumstances, it can be implied, express (e.g. health data) or written (e.g. data revealing ideology)

Unless the law requires express consent, the Data Protection Regulations established that data controllers can inform data subjects of the processing they intend to carry out and give them 30 days to oppose it. This way of obtaining consent is subject to limitations (consent can be requested only once a year for the same purpose).

Consent from a parent or guardian is needed for children under 14 years of age.

Data subjects' consent is not required when:

- Data is collected by a public administration when exercising its functions.

24 When collecting personal data, data subjects must be informed of:
The existence of a data file or data processing.
The data controller's identity and address (or its representative in case)
The purpose of the processing.
The data recipients, identifying them by name and address and specifying the purpose of the data transfer.
How the data subject can exercise his rights of access, rectification, cancellation and opposition.
Whether answering the questions is mandatory or voluntary (unless the information can be clearly inferred from the nature of the personal data requested or the circumstances in which the data is collected).
The consequences of providing the data or refusing to do so (unless the information can be clearly inferred from the nature of the personal data requested or the circumstances in which the data is collected).

- Data refers to the parties to an administrative, employment or business contract or pre-contract, provided the data is necessary for its performance.
- The purpose of the data processing is to protect the data subject's vital interest.
- The data processing is necessary to satisfy a legitimate interest pursued by the data controller (or a third party to whom the data is disclosed), provided that the data subject's fundamental rights and freedoms are not overridden.

Special rules apply to certain types of data, particularly to sensitive data. Sensitive data includes the following categories:

- Ideology, trade union membership, religion and beliefs. As a rule, this data can only be processed with the data subject's express written consent.
- Racial origin, health and sex life. As a rule, this data can only be processed on general interest grounds established by law, or with the data subject's express consent.
- Data related to administrative or criminal infringements, which can only be processed by the competent public administrations.

Data on ideology, trade union membership, religion, beliefs, racial origin, health and sex life can be processed when necessary for medical prevention or diagnosis, providing healthcare or medical treatment, or managing health services, provided that the processing is carried out by a healthcare professional bound by professional secrecy, or any another person subject to an equivalent obligation. This data can also be processed when necessary to protect a vital interest of the data subject or other person if the data subject is physically or legally unable to give consent.

As a rule, data on ideology, trade union membership, religion, beliefs, racial origin, health and sex life is subject to the high-level security measures established by the Data Protection Regulations.

3.3.4.4. Rights

Rights of individuals

When collecting personal data, data subject must be informed of:

- The existence of a data file or data processing.
- The data controller's identity and address (or that of its representative if the processing is carried out by a data controller not established in the EU but using means located in Spain, unless such means are used only for transit purposes).
- The purpose of the processing.
- The data recipients, identifying them by name and address and specifying the purpose of the data transfer.
- How the data subject can exercise his rights of access, rectification, cancellation and opposition.
- Whether answering the questions is mandatory or voluntary (unless the information can be clearly inferred from the nature of the personal data requested or the circumstances in which the data is collected).
- The consequences of providing the data or refusing to do so (unless the information can be clearly inferred from the nature of the personal data requested or the circumstances in which the data is collected).

Other granted rights:

- Right of access. Data subjects are entitled to request information on whether their personal data is processed, the purpose of the processing, the source of their data and

any data transfers, as well as information on specific data, data included in a specific file, or all the data that is subject to processing.

- Right to rectify incomplete or inaccurate data.
- Right of cancellation. Data subjects can request deletion of inappropriate or excessive data25.
- Right to oppose the data processing in specific scenarios established by law (e.g. receiving commercial communications).
- Right to challenge decisions that have a legal effect on them or that affect them significantly when the decision is exclusively based on automated data processing carried out to evaluate aspects of their personality (e.g. work performance and credit).
- Right to consult the General Data Protection Registry.
- Right to claim protection of their rights from the Data Protection Agency when they have been denied by the data controller.
- Right to be indemnified for damages caused by infringement.

3.3.4.5. Security Requirements / Notification / Third parties / Communication / Transfer

Security requirements

Data controllers and data processors must implement security measures to protect personal data against accidental or unlawful destruction, accidental loss, alteration or unauthorized disclosure or access.

The Data Protection Regulations set out specific minimum-security measures to be implemented by controllers and processors, establishing three cumulative security levels: basic, medium and high. The applicable measures depend on the nature of the data (e.g. sensitive data is subject to all three levels of security).

The security measures established by the Data Protection Regulations include specifications on:

- Access control.
- Identification and authentication.
- Incident records.
- Management of documents and media.
- Backup copies.
- Security officers.
- Audits.
- Access records.
- Telecommunications.

All measures must be described in a security document that also specifies the obligations of any employees, agents and contractors accessing the data files, and the structure of the files, including a description of the systems processing them.

Notification

There is no requirement to notify data security breaches under the Data Protection Act or the Data Protection Regulations Acknowledging guilt for a specific breach will be taken into

25 Data controllers must cancel personal data when it is no longer necessary or relevant to the purpose for which it was collected. Cancellation means that the data cannot be used and must be blocked to impede its processing. It is kept available for public administrations, judges and courts to deal with any liabilities resulting from the processing until these liabilities expire. After any applicable liabilities expire, the data must be deleted.

consideration by the Data Protection Agency when imposing penalties. Notifying data subjects can also reduce civil liability.

The General Telecommunications Act establishes an obligation on telecoms operators to notify the Data Protection Agency without delay of any personal data breach. This Act defines personal data breaches as any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored or processed in connection with the provision of a publicly available electronic communications service.

Processing by third parties

When a company processes personal data by providing a service to the data controller, the data processing must be regulated by contract, specifying that the processor must:

- Process the data only in accordance with the data controller's instructions.
- Not apply or use the data for purposes other than those established in the contract.
- Not communicate the data to third parties.
- Implement the appropriate security measures.

Data processors can communicate the data to others when authorized by the data controller. The Data Protection Regulations establish the conditions under which the main data processor can sub-contract part of the services rendered to the data controller if the sub-contractor can also process the data.

Electronic communications

Under the Information Society Services Act, information society services providers can use cookies and equivalent devices in users' equipment if the users consent to it. Users must first be provided with clear and complete information about the use of such devices, particularly with regard to data processing.

This requirement does not apply when the only purpose of the device installed in the users' equipment is to transfer information via electronic communication networks, or when using the device is necessary to provide a service expressly requested by the user.

Under the Data Protection Agency's guidelines (which are not mandatory but should be followed by information society service providers/data controllers since they reflect how the Agency interprets the rules) users must be informed of cookies (and equivalent devices) using two layers:

- The first layer (usually a pop-up) must briefly inform the user about the cookies, identifying their purpose and whether they are first or third-party cookies. This layer must include an accept button or warn users that a specific action (like continuing to use the site) will imply acceptance of the cookies. It must also include a link to the second layer.
- The second layer must include detailed information about cookies: definition, types of cookies and their purpose, how to disable or eliminate them and reject their use, and identification of third parties when third party cookies are used.

Requirements for sending unsolicited electronic commercial communications (spam)

Recipients must consent to receiving electronic commercial communications. An opt-out is valid for communications relating to first party products or services like those initially requested by the customer. An opt-on is required when communications relate to third party products or services, or products or services other than those initially requested by the customer.

International transfer of data.

Transfer of data outside the jurisdiction

International data transfers are transfers to countries whose level of protection has not been declared adequate by the relevant authorities (any country outside the European Economic Area (EEA) with some exceptions). Such transfers must be notified to the Data Protection Agency and authorized by its director, regardless of whether the data importer belongs to the same group as the data exporter.

Authorisation can be obtained using the Model Contracts for the transfer of personal data to third countries approved by the European Commission[26].

The Data Protection Agency must receive the contract and confirm that the parties' representatives have sufficient power to sign it. The Agency has up to three months from the date it receives the request to issue and communicate its decision.

Data Protection Agency authorization is not necessary in the following cases (although it must still be notified of the international data transfer):

- When the transfer results from the application of an international treaty to which Spain is party.
- When the transfer is meant to provide or request international judicial aid.
- When the transfer is necessary for medical prevention or diagnosis or providing healthcare or medical treatment or for managing healthcare services.
- When the transfer relates to money transfers made according to their specific legislation.
- When the data subject has unequivocally given consent to the data transfer (if the data subject has no real option to oppose the transfer (which is usually the case with employees) consent will not be valid).
- When the transfer is necessary for performance of a contract between the data subject and the data controller or to adopt pre-contractual measures at the data subject's request.
- The transfer is necessary to execute or perform a contract concluded or to be concluded, between the data controller and a third party in the interest of the data subject.
- When the transfer is necessary or legally required to protect the public interest.
- When the transfer is necessary for the recognition, exercise or defence of a right in a legal proceeding.

There is no requirement to store personal data inside the jurisdiction.

3.3.4.6. Enforcement and sanctions

The Data Protection Agency is responsible for imposing sanctions for non-compliance and it is entitled to inspect data files and request any information necessary to perform its functions. The Data Protection Agency's inspectors can ask to see documents and data and examine them wherever they are located, as well as check out the physical equipment and software used to process data by accessing the premises where it is installed.

Data protection infringements can be classified as:

26 The Data Protection Agency has approved standard contractual clauses that regulate international data transfer from a data processor established in Spain to data sub-processors established in countries whose level of protection is not adequate. In this case, to obtain the Data Protection Agency's authorization, the data processor must also provide the Data Protection Agency with an agreement between the data processor and the data controller under which the latter authorizes the sub-contracting and the international data transfer.

- Minor infringements. These are subject to fines ranging from 900€ to 40.000€.
- Serious infringements. These are subject to fines ranging from 40.001€ to 300.000€.
- Very serious infringements. These are subject to fines ranging from 300.001€ to 600.000€.

Sanctions are graduated in proportion according to the following circumstances:

- Continuous nature of the infringement.
- Volume of processing.
- Connection between the infringer's activity and the data processing.
- Infringer's business/activity volume.
- Benefits obtained as a result of the infringement.
- Degree of intention.
- Reoccurrence.
- Nature of the damages caused to the data subjects or third parties.
- Whether the infringer had adequate processing procedures and the infringement was the result of an anomaly, rather than lack of diligence.
- Any other relevant circumstances to determine the degree of guilt.

Lower sanctions are imposed (for example, a serious infringement would be sanctioned as if it were a minor infringement) when:

- Several of the above circumstances occur.
- The infringer diligently rectifies the situation.
- The infringer's behaviour may have induced the infringement.
- The infringer spontaneously acknowledges its guilt.
- There is a merger by absorption, and the infringement was committed before the merger and cannot be attributed to the absorbing company.

In some cases, after hearing the parties and considering the facts, the Data Protection Agency can replace fines with a warning giving the infringer time to prove that it has taken the necessary corrective measures. This applies if it is the first infringement and if it is not very serious.

When the infringement is serious or very serious and persisting with the data processing can cause serious damage to the data subjects' fundamental rights (particularly, data protection rights), the Data Protection Agency can order data controllers to cease processing. If this request is disregarded, the Data Protection Agency can decide to freeze the corresponding data files.

The Data Protection Agency is especially active in prosecuting infringements. In 2014, it resolved 12.173 claims and complaints, issued 872 sanctioning decisions, and imposed fines of 17,3k€.

3.3.4.7. Spanish Data Protection Agency

Agencia de Protección de Datos

C/Jorge Juan, 6
28001 Madrid
Tel. +34 91399 6200
Fax +34 91455 5699
e-mail: internacional@agpd.es
Website: https://www.agpd.es/

- Art 29 WP Member: Ms María del Mar España Martí, Director of the Spanish Data Protection Agency
- Art 29 WP Alternate Member: Mr. Rafael Garcia Gozalo

3.4. Data Protection Protocol WellCo

3.4.1. Members of the WellCo Project and Personal Data that will be processed.

3.4.1.1. Members

Project partners must be distinguished between Public Administrations and private entities. Although the generic Data Protection regulations are applicable to both sectors, we must take into account the different modalities that must be met by Public Administrations, well established in the general regulations themselves, as well as in some of the existing sectoral regulations.

Processing has started at the time of preparing this report, with the so-called "Phase 1- pilot project", in which small groups of subjects are participating in pilot projects in the different countries.

Pilot projects are being carried out in each of the countries by persons belonging to public entities, for which the data processing is protected by pre-established data protection protocols present in those organisms. However, due to the qualification of the data, and because it is treated differently, the informed consent of the participants must be obtained as established in the national regulations applicable to each of the public entities.

3.4.1.2. Different phases

	Data processing phases
Phase 1	The data processing of the WellCo project can be differentiated into two phases. The first one, consists on the pilot projects (already exposed throughout the report) that are being carried out by 3 project partners, located in Spain, Italy and Denmark (and in some cases, specific collaborators). In each of these countries, the different national application rules are being complied with. The requirements for compliance will be set forth in paragraph 1.4 of this Section
Phase 2	The second phase will be the validation of the WellCo platform. The platform will be tested by a high number of participants, without considering large-scale or mass personal data processing. It will start once the R (EU) 679/2016 has entered into force and therefore it must be complied with, also considering the fact that although the proceedings initiated before the Regulation are exempt from its immediate application, the recommendation of WP 29 is to review and, if applicable, extend data protection in accordance with the referenced Regulation.

Table 6.- Data Processing Phases

3.4.1.3. Data Qualification

Common bases to all project partners:

- Type of personal data.

- Personal data subjects.
- How are project partners going to collect the personal data.
- How will personal data be processed.
- Data transfer.

3.4.2. Applicability of Regulation

The state regulation is of direct application during the first phase and of subsidiary application in the second one.

3.4.2.1. Denmark

Denmark	
Phase 1	For phase 1, the following national regulation applies: • Act of Processing Personal Data. • General Authorization for Public Research. Regarding the applicable regulation, in addition to the General Authorization previously mentioned, the first phase of the WellCo Project is covered by the General Authorization given by the Danish Data Protection Agency, and it is sufficient to comply with the Data Protection Protocol by obtaining an informed consent from all the participants to process the relevant data for the present project (Appendixes- Informed consent for participants)
Phase 2	From 25 May 2018, Regulation (EU) 679/2016 will be in force and applicable to all members of the WellCo Project. In attention to the new regulation and in absence of any white list given by the National Supervisory Authorities, a DPIA should be conducted (according to the Guidelines and recommendations given by WP 29, although it could be considered that the WellCo project will not process data according to more than two of the given criteria that entails required DPIA).

Table 7.- Denmark: phases and applicable regulation

3.4.2.2. Italy

Italy	
Phase 1	For phase 1, the following national regulation applies: • Legislative Decree No. 196/2003, Italian Data Protection Code. • Authorization No. 2/2014 Concerning Processing of Data Suitable for Disclosing Health or Sex Life. • Authorization no. 9/2016 General Authorization to Process Personal Data for Scientific Research Purposes. In attention to the applicable legislative decree and the general authorization referred to it is sufficient to give compliance to data protection by obtaining the data subject's written consent (available in the WellCo repository Alfresco). According to the general authorization, there is no obligation to prior notification of the processing of personal data, because all data is anonymized, SMS/Images are recorded only by local participants' own technical devices and gathered during the interviews. Each participant

	will be assigned a numeric code, which substitutes and encrypts the name and other personal references.
Phase 2	From 25 May 2018, Regulation (EU) 679/2016 will be in force and applicable to all members of the WellCo Project. In attention to the new regulation and in absence of any white list given by the National Supervisory Authorities, a DPIA should be conducted (according to the Guidelines and recommendations given by WP 29, although it could be considered that the WellCo project will not process data according to more than two of the given criteria that entails required DPIA).

Table 8.- Italy: phases and applicable regulation

3.4.2.3. Spain

Spain	
Phase 1	For phase 1, in order to comply with the Spanish regulations regarding the Organic Law of Protection of Personal Data (Ley Orgánica de Protección de Datos de Carácter Personal, LOPD), the legal entity/ legal person must: • Register the files of personal data that will be treated. • Ensure that the data are adequate and truthful, lawfully and lawfully obtained, and treated in a manner commensurate with the purpose for which they were collected. • Save the secret and security. • Inform the owners of the personal data in the collection of these and obtain the consent for the treatment of the personal data • Facilitate and guarantee the exercise of the rights of the subject (opposition, access, rectification and cancellation) • Ensure that in its relations with third parties providing services, which carry access to personal data, the requirements of the LOPD are fulfilled. There are No conduct codes of personal data processing ex article 32 LOPD to which the project WellCo or one of its members could be accommodated. Prior to the processing of data, the participants have given their consent having been informed about the project, of their different rights and the corresponding treatment of personal data, all in attention to the provisions of the Organic Law 15/1999, of 13 December, protection of personal data. All the above expresses attention to what it was stated in judgment of 15 June 2001 by the National Court: *"This is a very important right* [that of information to the subject of personal data] *because it is the one that allows to carry out the exercise of other rights, and thus it values the positive text to detail its content and to establish the requirement that it be express, precise and unequivocal. And of the provisions of article 5 of the LOPD".* Article 6.1: "1. The processing of personal data shall require the unequivocal consent of the person concerned, unless otherwise provided by law. "

However, Article 6.2 adds that

"(...) consent shall not be required where personal data are collected for the exercise of the functions of public administrations in the field of their competencies; where they refer to the parties to a contract or to a contractual, labour or administrative relationship and are necessary for their maintenance or compliance; Where the processing of the data is intended to protect a vital interest of the person concerned in the terms of article 7 (6) of this law, or where the data appear in sources accessible to the public and its treatment is necessary for the satisfaction of Legitimate interest pursued by the person responsible for the file or by the third party to whom the data is communicated, provided that the rights and fundamental freedoms of the person concerned are not violated."

The regulation of development of the Organic Law 15/1999, approved by the Royal Decree 1720/2007, of 21 December, specifies in its article 10.3 that

"the data of personal character can be treated without the consent of the interested person when:

Are collected for the exercise of the functions of the public administrations in the field of competences attributed to them by a standard of law or a standard of Community law.

They are refitted by the person in charge of the treatment on the occasion of the conclusion of a contract or pre-agreement or of the existence of a trade, labour or administrative relation of which the affected one is part and are necessary for its maintenance or fulfilment."

In the case of the WellCo project, the data obtained are already registered as part of the existing data protection files of the respective partners. In addition, informed consent of the data subject shall be required (informed consent available in WellCo repository, Alfresco).

Finally, the communication of data by the person who obtained it from external companies collaborating in the provision of social services constitutes a transfer of personal data, defined in article 3 (i) of the LOPD, as:

"Any disclosure of data made to a person other than the interested party".

Such a transfer must be subjected to the general system of communication of personal data established in article 11 of the same law, which establishes that it can only be verified for the fulfilment of purposes directly related to the legitimated functions of the assignor and assignee and requires, in order that it may take place, the consent of the person concerned (article 11.1), granted prior to the transfer and sufficiently informed of the purpose to which the data whose communication is authorized or the Type of activity of the one to whom it is intended to communicate (art. 11.3), and which must obtain the assignor as responsible for the file that contains the data that is intended to cede.

Phase 2

The second phase will begin once the Regulation (EU) 679/2016, of 27 April (hereinafter the GDPR) has come into force and must therefore be complied with as established therein. In the case of Spain, it is also necessary to take into account the draft law on data

protection, which may be adopted simultaneously and which, at some points, is referred to in the European regulation.

The data to be treated by the members of the WellCo project are considered "sensitive personal data" accordingly to article 9 of the Rules of Procedure, so all security measures must be taken to safeguard the integrity of the personal data of the Participants.

Therefore, in order to comply with the provisions of the European Data Protection regulation, one of the key elements for the activity of the WellCo project is the informed consent of the participants, which must be obtained prior to the beginning of the Processing of personal data, in the context of article 6 in relation to article 9 of the GDPR.

The informed consent will be, as mentioned before, essential for any treatment of data in attention to the sensitivity and qualification of the same. Such consent must be freely provided, specifically for the particular treatment, and contain sufficient information for the subject to understand the scope and object of prosecution, as well as the rights facing the processing.

To ensure compliance with data protection, the Informed consent for participants must collect (see WellCo informed consent example in Appendix):

- The identity of the responsible (controller).
- The purpose of each of the processing operations for which consent is sought.
- The type of data to be collected and used.
- The existence of the right to withdraw consent.
- The possible risks of data transfer to third countries in the absence of an adequacy decision and appropriate safeguards (if the consent relates to transfer).
- Expressly with the faculty of Cession of the data in a pseudonymized way or totally anonymized to the different partners of the project. In addition, the duration of the data processing must be expressly stated, and if, if necessary, at the end of the study, these data will be provided fully anonymized to third parties or definitively eliminated.

The project does not envisage obtaining data from third parties, unless it is Open data or totally anonymous data sets, so unless the assignor indicates otherwise, these data are not considered covered by the GDPR.

In particular, in the case of the public entities in Spain there are registered files that cover the action so far, since the participants are normally assisted by at least one of the partners of the project. However, a specific consent must be obtained for the processing of personal data during the investigation of the project, providing the participants with the information previously reviewed. This consent has been obtained in writing and is included in the project documentation (Appendixes- Informed consent for participants).

	Apart from the specific regulation of the LOPD, public entities in Spain must comply with a number of requirements established in the sectoral regulations such as: • Law 40/2015, of 1 October, on the legal system of the public Sector • Law 39/2015, of 1 October, on the common administrative procedures of the public administrations • Law 19/2013, of 9 December, on transparency, access to public information and good governance • Law 37/2007, of 16 November, on reuse of the information of the public sector • Royal Legislative Decree 3/2011, of 14 November, approving the revised text of the law of contract of the public Sector • Real Decree 4/2010, of 8 January, which regulates the national scheme of interoperability in the field of the electronic administration • Royal Decree 3/2010, of 8 January, which regulates the national security scheme in the field of the electronic administration • Royal Decree 1671/2009, of 6 November, which partially develops the law 11/2007, of 22 of June, on electronic access of the citizens to the public services Since all the regulation must be fulfilled by the normal functioning of the public entities involved in the project, no modification or measures to be taken for the implementation of the pilot project are required in the Spanish case

Table 9.- Spain: phases and applicable regulation

3.4.3. Data Protection Protocol and Guidelines

3.4.3.1. Data controller

Data 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law," Article 4, 7

The controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with article 24, 25, 30, 31 and 32 GDPR.

Therefore, the controller must:

- Keep a backup copy and data recovery procedures in a different place from where the computer equipment that deals with them is, which must comply with the security measures required by GDPR, or using elements that guarantee the integrity and recovery of information, so that recovery is possible.
- Establish the opportune measures so that exclusively the personnel authorized has access to the places where the physical equipment that supports the information systems is installed.

- Proceed to the destruction or deletion of any document or medium containing personal data that is to be discarded, adopting the measures to prevent any subsequent recovery of the information.
- Make a backup prior to real-life tests.
- Establish a notification and incident management procedure with indication of: type, date-time, person notifying, to whom it is communicated and effects that produce.
- Establish access controls for users in such a way that they only have authorized access to data and resources necessary for their functions.
- Ensure that, prior to the implementation or modification of the information systems, the tests are not carried out with real data, unless the level of security corresponding to the type of file treated is ensured.
- Periodically review the registered control information and prepare a report of the reviews carried out and the problems detected at least every month.
- Make sure that the mechanisms that allow the registration of the data detailed in the previous paragraphs are under the direct control of the data controller or security officer, without allowing in any case the deactivation of the same.
- Adopt measures so that, for each access will be recorded, at least: identification of the user, date and time it was made, file accessed, type of access and if it has been authorized or denied.
- In the case that the access has been authorized, the information that allows identification of the accessed must be registered.
- Have an updated list of users with authorized access to the information system, with identification and authentication procedures for such access.
- The person in charge of the data will be responsible for verifying every six months the correct definition, operation and application of the procedures for making backup copies and recovering the data.
- Document the functions and obligations of personnel.
- Proceed to the destruction of copies or reproductions of discarded materials in a manner that avoids access to the information contained in them or their subsequent recovery.
- Adopt appropriate measures so that users' access is limited to the resources they need to carry out their functions.
- Draft and review the existence of a procedure that indicates how to proceed with the destruction of discarded copies or reproductions that contain high level data in a way that prevents access to information.
- Identify the type of information contained in the media and documents that contain personal data.
- Establish mechanisms to prevent a user from accessing non-automated files with rights other than those authorized.
- Establish a procedure so that when the physical transfer of the documentation with high-level data contained in files is carried out, measures are taken to prevent access.
- They can be cryptically labelled (only understandable for users with authorized access) when they contain personal data that the organization considers especially sensitive.
- They will not be tagged when the physical characteristics of the support make it impossible to comply with them, and a written record of this will be provided in the protocol document.
- Adopt measures so that media and documents containing personal data are only accessible by the personnel authorized for this in the security document.

- Adopt the measures so that only the authorized personnel in the security document can grant, alter or cancel authorized access to non-automated files, in accordance with the criteria established by the person responsible for the file.
- Periodically review the record of access to high-level data contained in documents.
- Establish a record in which the type of incident is recorded, the moment in which it occurred, or where appropriate, detected, the person who makes the notification, to whom it is communicated, the effects that would have been derived from the same and the corrective measures applied, in relation to the non-automated files.
- Document the functions and obligations of personnel in relation to non-automated files.
- Arrange the opportune measures so that the supports or documents are archived in agreement with criteria that guarantee the correct conservation of the documents, the location and consultation of the information and make possible the exercise of the rights of opposition to the treatment, access, rectification and cancellation.
- Submit information systems, at least every 2 years, to an internal or external audit that verifies compliance with the security measures required for non-automated files.
- The exit of media and documents that contain personal data, outside the premises under the control of the person responsible for the file or treatment must be authorized by the person responsible for the file or be duly authorized in the security document.
- Prepare and maintain an up-to-date list of users and user profiles for non-automated files, and the authorized accesses for each of them.
- Analyse the audit report and raise the conclusions to the person responsible for the file so that it adopts the appropriate corrective measures and will remain available of the Data Protection Agency.
- Adopt appropriate measures so that third-party personnel who have access to non-automated files are subject to the same security conditions and obligations as their own personnel.
- Establish a mechanism that limits the possibility of repeatedly trying unauthorized access to the information system.
- Create and maintain an entry record of computer media with indication of: type of support, date and time, issuer, number of media, type of information they contain, shipping form and responsible for the reception (which must be duly authorized).
- Create and maintain an output record of computer media with indication of: type of support, date and time, recipient, number of media, type of information they contain, shipping form and responsible for delivery (which must be duly authorized).
- Arrange what is necessary so that only authorized personnel can grant, alter or cancel authorized access, according to the criteria established by the person responsible for the file.
- Submit the information systems, at least every 2 years, to an internal or external audit that verifies compliance with the Regulation, procedures and instructions.
- Adopt technical and organizational measures so that the distribution of media will be done by encrypting the data or using another mechanism that ensures that the information is not intelligible or manipulated during transport.
- Extraordinarily carry out this audit whenever substantial changes are made to the information system that may affect compliance with the security measures implemented in order to verify the adaptation, adequacy and effectiveness of the same.

- Establish a mechanism that allows the unambiguous and personalized identification of any user that tries to access the information system and the verification that it is authorized.
- Adopt the technical and organizational measures so that the transmission of personal data through public networks or wireless telecommunications networks is done by encrypting said data or using any other mechanism that guarantees that the information is not intelligible or manipulated.
- Make sure that the computer supports are inventoried and stored in a place with restricted access to the authorized personnel in the security document. (NOTE: These obligations are excepted when the physical characteristics of the support make it impossible to comply with them, with proof of this in the security document).
- Define the functions and obligations of the staff.
- Appoint the responsible security officers and adopt the necessary measures so that the Security Managers know the security rules that affect the performance of their functions as well as the consequences that could be incurred in case of non-compliance.
- In case of authentication with passwords, define and implement an allocation, distribution and storage procedure that guarantees its confidentiality and integrity.
- Take care that the registry records the procedures performed to recover the data, indicating the person who executed the process, the restored data and, where appropriate, what data it was necessary to manually record in the recovery process.
- Obtain written authorization from the person responsible for the file for the execution of the data recovery procedures.
- Make backup copies, at least weekly, unless in that period there was no update of the data.
- Authorize data recoveries.
- Adopt the necessary measures so that the users of your organization are aware of the security norms that affect the performance of their functions as well as the consequences that may be incurred in case of non-compliance.
- Establish mechanisms to prevent a user from accessing data or resources with rights other than those authorized.
- Check that passwords are changed periodically and their storage is unintelligible while they are in force.
- Review the periodic controls to verify compliance with the provisions of the protocol document.
- Implement (or, where appropriate, modify) periodic controls to verify compliance with the provisions of the protocol.
- Keep the recorded data for two years.
- Authorize the exit of supports outside the premises.
- Adopt the necessary measures so that those responsible for security know the security rules that affect the development of their functions as well as the consequences that could be incurred in case of non-compliance.
- Check that only authorized personnel can access high-level paper information.
- Establish mechanisms to identify the accesses made in the case of documents that contain high-level data that can be used by multiple users.
- Update the list of authorized personnel to access personal data on high-level paper.
- Inventory the supports and documents that contain personal data.
- Establish a notification and management procedure for incidents related to non-automated files.

- Take care that the areas where the cupboards and filing cabinets are located that contain information with high level personal data remain closed when access to the documents they contain is not necessary. (Unless the characteristics of the premises were not possible to have closed areas in which case the responsible will adopt alternative measures that, duly motivated, will be included in the security document).
- Update the list of authorized persons to make copies of information that contains high-level data.
- Take care that storage devices for documents containing personal data have mechanisms that hinder their opening. (When the physical characteristics of those do not allow adopting this measure, the person in charge of the file or treatment will adopt measures that prevent the access of unauthorized persons, a measure that may consist in the custody of the person who is in charge).
- Define the functions and obligations of personnel in relation to non-automated files.
- Appoint and replace, if applicable, the appropriate security officers (responsible for coordinating the security measures of non-automated files).
- Check that only authorized persons in the security document make copies of documents containing high-level data.
- Ensure that cabinets and filing cabinets containing information with high level personal data are in areas where access is protected with access doors equipped with key-opening systems or another equivalent device.
- Have the consent (depending on the case: express or express and in writing) for the treatment of sensitive data.
- Check that, except in the cases in which the Law exempts this obligation, you have the prior, free and informed consent of the owner of the data for the processing of your data.
- Check that the personal data object of treatment is not used for purposes incompatible with those for which the data had been collected.
- Check that the personal data are accurate and updated so that they respond truthfully to the current situation of the affected.
- Detect the assumptions of those in charge of the treatment and check the subscription of the treatment manager contracts.
- Check the fulfilment of the information duty.
- Check that the data processed are adequate, relevant and not excessive in relation to the scope and the specific, explicit and legitimate purposes for which they were obtained.
- Implement (and if necessary revise and / or modify) the procedure for the attention to the holder of the data in the exercise of rights of access rectification, cancellation and opposition.
- Order the timely cancellation so that personal data are cancelled when they are no longer necessary or relevant for the purpose for which they were collected or recorded or when they prove to be inaccurate, in whole or in part, or incomplete and review the correct execution of this obligation.
- Address requests for the exercise of rights of access rectification, cancellation and opposition.
- Verify that, except in the cases in which the Law exempts this obligation, prior, free and informed consent of the owner of the data for the transfer of data is available.
- Detect the suppositions of provision of services without access to data and check the subscription of contracts to prohibit access to data.

WellCo can be considered as a "**Cross-border processing of personal data"**, because the processing of personal data takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State.

Also, the processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State constitute cross-border processing (Article 4 (23) GDPR).

This consideration is relevant to identify the lead supervisory authority, which is the authority where the project establishes the main establishment. To identify the main establishment, it is firstly necessary to identify the central administration of the data controller in the EU, or where the effective and real exercise of management activities, that determine the main decisions as to the purposes and means of processing through stable arrangements, takes place.

WellCo might designate more than one data controller, so that more data controllers will be operating jointly. In case of Joint Controllers with establishments in the EU, the controllers shall in a transparent manner determine their respective responsibilities for compliance with their obligations under the Regulation.

The joint controllers should designate (among the establishments where decisions are taken) which establishment of the joint controllers will have the power to implement decisions about the processing with respect to all joint controllers. This establishment will then be considered to be the main establishment for the processing carried out in the joint controller situation. The arrangement of the joint controllers is without prejudice to the liability rules provided in the GDPR, in particular in Article 82 (4).

At the time of the elaboration of the present deliverable, before the GDPR comes into force, neither a data controller of WellCo project is appointed, nor the main establishment of the data processing. Based on the GDPR further actions will be taken in the project if needed in order to identify the mentioned roles.

3.4.3.2. Data processors

Data Processor: "means a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller. Article 5, 8 GDPR.

The obligations are established in article 28 GDPR, the processor depends directly from the authorizations and instructions from the data controller, and should:

- Save the necessary secrecy regarding any type of information of a personal nature known in function of the work carried out, even after the employment relationship with the organization is concluded.
- Save all physical media and / or documents that contain information with personal data in a safe place, when they are not used, particularly outside the working day.
- It is prohibited to transfer any support, list or document with personal data in which information belonging to the organization is stored outside the premises of the same, without prior authorization of the Security Manager. In the event of transfer or distribution of media and documents, this will be made by encrypting the data, or by another mechanism that prevents access or manipulation of information by third parties.
- Files of a temporary nature or copies of documents are those in which personal data are stored, generated for the fulfilment of a specific need or temporary and auxiliary works, as long as their existence does not exceed one month. These temporary files or copies of documents must be deleted once they are no longer needed for the purposes that

led to their creation and, while they are in force, must meet the security levels assigned by the Security Manager. If, after the month, the user needs to continue using the information stored in the file, he / she must inform the Security Manager to take the appropriate measures on it.

- Only authorized persons in a list of accesses may enter, modify or cancel the data contained in the files or documents subject to protection. The access permissions of the users are granted by the Security Manager. In the case that any user requires, for the development of their work, access to files or documents whose access is not authorized, you must inform the corresponding Data Controller or Security Officer.
- Notify the Data Controller or Security Manager, in accordance with the notification procedure, of security incidents he/she is aware of.
- Change the passwords at the request of the system.
- Close or block all sessions at the end of the working day or in the case of temporarily absent from work, to avoid unauthorized access.
- Do not copy the information contained in the files in which personal data is stored to the personal computer, diskettes, laptop or any other medium without the express authorization of the corresponding Security Manager.
- Save all the files with personal data in the folder indicated by the corresponding Security Manager, in order to facilitate the application of security measures that correspond to them.
- Users are prohibited from sending high-level personal information, unless expressly authorized by the Security Manager assigned to this task. In any case, this shipment can only be made if the necessary mechanisms are adopted to prevent the information from being intelligible or manipulated by third parties.
- The users will not be able to install any type of computer programs or devices neither in the central servers nor in the computer used in the job, unless expressly authorized by the Security Manager assigned to this task.
- It is forbidden:
    - To use identifiers and passwords of other users to access the system.
    - To try to modify or access the access registry enabled by the competent Security Manager.

3.4.3.3. Informed consent

For consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. Therefore, WP29 has recommended that at least the following information would be required for obtaining valid consent:

- The controller's identity
- The purpose of each of the processing operations for which consent is sought
- The (type of) data that will be collected and used
- Duration of data processing
- The existence of the right to withdraw consent
- Right to lodge a complaint with a supervisory authority
- Right to request access to and rectification or erasure of personal data or restriction of processing concerning the data subject, as well as the right to data portability
- Information about the use of the data for decisions based solely on automated processing, including profiling, in accordance with Article 22 (2) [not applies to WellCo]

- If the consent relates to transfers, about the possible risks of data transfers to third countries in the absence of an adequacy decision and appropriate safeguards (Article 49 (1a)) [not applicable to WellCo]

With the abovementioned specification, an Informed Consent for WellCo project under the GDPR has been elaborated (see Appendix I)

3.4.3.4. Data Protection Impact Assessment (DPIA)

According to the WP29 Guidelines, a DPIA is not clearly required, but highly recommended. In attention of the ambiguous determination of cases in article 35 GDPR and the Guidelines established by WP29, the WellCo Project could be considered as a profiling data processing including sensitive data, and in conclusion the recommendation is to carry out a DPIA, as it is a useful tool to help data controllers comply with data protection law.

The DPIA should contain:

- A systematic description of the envisaged processing operations and the purposes.
- An assessment of the necessity and proportionality of the processing in relation to the purposes.
- An assessment of the risks for individuals and
- The measures in place to address the risks, including safeguards, security measures and mechanisms to demonstrate compliance.

According to Article 35 (1), it is the task of the controller, not of the DPO, to carry out, when necessary, a DPIA. However, the DPO can play a useful role in assisting the controller.

The DPIA may concern a single data processing operation, but according to article 35 (1) a single assessment may address a set of similar processing operations that present similar high risks. This means that a single DPIA could be used to assess multiple processing operations that are similar in terms of the risks presented, provided that adequate consideration be given to the specific nature, scope, context and purposes of the processing. When the processing operations involve joint controllers, they need to define their respective obligations precisely. The DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights of the data subjects.

The GDPR does not require a DPIA to be carried out for every processing operation, which may result in risks for the rights and freedoms of natural persons. Carrying out of a DPIA is only mandatory where a processing is likely to result in high risks to the rights and freedoms of natural persons.

Article 35 (3) provides some examples when a processing is *"likely to result in high risks":*

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

According to the guidelines provided by WP29, the following criteria should be considered to determine necessary a DPIA:

- Evaluation or scoring.
- Automated-decision making with legal or similar significant effect.
- Systematic monitoring.
- Sensitive data.

- Data processed on a large scale.
- Data concerning vulnerable data subjects.
- Innovative use or applying technological or organizational solutions.
- Data transfer across border outside the European Union.

If the processing could provide a high-level risk for personal data, or at least two of these criteria are fulfilled, a DPIA is required.

The requirement to carry out a DPIA applies to processing operations meeting the criteria in Article 35 and initiated after the GDPR becomes applicable on 25 May 2018.

WP29 recommends carrying out a DPIAs for processing operations already underway prior to May 2018. In addition, where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operation. This could be the case when a new technology has come into use or because personal data is being used for different purposes, so that it can be considered a new data processing operation and could require a DPIA.

In a DPIA the controller must seek the views of data subjects or their representatives, where appropriate, the WP29 considers that:

- Those views could be sought through a variety of means, depending on the context.
- If the data controller's final decision differs from the views of the data subjects, its reasons for going ahead or not should be documented.
- The controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate.

The GDPR sets out the minimum features of a DPIA (Article 35 (7), recitals 84 and 90):

- A description of the envisaged processing operations and the purposes of the processing.
- An assessment of the necessity and proportionality of the processing.
- An assessment of the risks to the rights and freedoms of data subjects.
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned

Recital 90 of the GDPR outlines several components of the DPIA which overlap with well-defined components of risk management. In risk management terms, a DPIA aims at managing risks to the rights and freedoms of natural persons, using the following three processes by:

- Establishing the context
- Assessing the risks
- Treating the risks

Publishing a DPIA is not a legal requirement of the GDPR. It is left upon the controller's decision, but he/she should consider publishing the DPIA or part, to demonstrate accountability and transparency. The published DPIA does not need to contain the whole assessment, especially when a DPIA could present specific information concerning security risks for the data controller or give away trade secrets or commercially sensate information.

In case a DPIA reveals high residual risks, the data controller will be required to seek prior consultation for the processing from the supervisory authority.

3.4.3.5. *Designation of Data Protection Officer*

Under the GDPR, it is mandatory for certain controllers and processors to designate a DPO. This will be the case for all public authorities and bodies (irrespective of what data they process), and for other organizations that, as a core activity, monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale.

Even when the GDPR does not specifically require the appointment of a DPO, organizations may sometimes find it useful to designate a DPO on a voluntary basis.

According to WP 29 the DPO is a cornerstone of accountability and appointing a DPO can facilitate compliance and furthermore, become a competitive advantage for businesses. In addition to facilitating compliance through the implementation of accountability tools (such as facilitating or carrying out data protection impact assessments and audits), DPOs act as intermediaries between relevant stakeholders like supervisory authorities, data subjects etc.

DPOs are not personally responsible in case of non-compliance with the GDPR. The Regulation makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24 (1)).

To sum up, there is no obligation to designate a Data Protection Officer for private entities, but article 37 GDPR establishes: "The controller and the processor shall designate a data protection officer if the processing is carried out by a public authority or body, except for courts acting in their judicial capacity." Consequently, the public bodies partners of WellCo Project should designate a DPO accordingly to art. 37 to 39 of the GDPR.

Although the GDPR does not define what constitutes a public authority or body, it includes national, regional and local authorities, and the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law. In such cases, the designation of a DPO is mandatory.

A public task may be carried out, and a public authority may be exercised not only by public authorities or bodies but also by other natural or legal persons governed by public or private law, according to national regulation of each Member State.

Even though there is no obligation in such cases, the WP29 recommends, as a good practice, that:

- Private organizations carrying out public tasks or exercising public authority designate a DPO.
- Such a DPO's activity should also cover all processing operations carried out, including those that are not related to the performance of a public task or exercise of official duty.

Article 37 (1) (b) and (c) requires that the processing of personal data be carried out on a large scale for the designation of a DPO to be triggered. The GDPR does not define what constitutes large-scale, but WP29 recommends that the following factors are considered when determining whether the processing is carried out on a large scale:

- The number of data subjects concerned.
- The volume of data and/or the range of different data items being processed.
- The duration, or permanence, of the data processing activity.
- The geographical extent of the processing activity.

The notion of regular or systematic monitoring of data subjects is not defined, but according to recital 24 it includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising. WP29 interprets regular as ongoing at intervals, recurring at fixed times and/or constantly. WP29 also interprets systematic as occurring according to a

system, pre-arranged and methodical, taking place as part of a general plan for data collection, carried out as part of a strategy. WP29 cites as an example in the guidelines: "monitoring of wellness, fitness and health data via wearable devices", which includes the WellCo Project.

The DPO *"shall be designated on the basis of professional qualities and expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39"* (Article 37 (5).

So DPO should fulfil:

- Level of expertise in attention to the data processing, sensitivity, complexity and amount of data.
- Professional qualities, expertise in national and European data protection regulation, as well as knowledge of the business sector of the data controllers' organization.
- Ability to fulfil its tasks.
- Based on a service contract.

Controller and processor are obligated to publish the contact details of the DPO and to communicate the contact details to the relevant supervisory authorities.

The DPO shall be involved in all issues relating to data protection. In relation to data protection impact assessments, the GDPR explicitly provides for the early involvement of the DPO and specifies that the controller shall seek the advice of the DPO when carrying out such impact assessments. The DPO should be informed and consulted at the outset to facilitate compliance with the GDPR. DPO shall:

- Be invited to participate in meetings of the management.
- Take part in decisions with data protection implications.
- Give his/her opinion about decision in relation to data protection issues.
- Be consulted in case of data breach or another incident.

The DPO shall receive necessary support and sufficient time to fulfil his/her duties.

The tasks of the DPO are monitoring compliance with GDPR (collect information to identify processing activities, analyse and check the compliance, inform, advise and issue recommendations to the controller or processor.

In accordance with the provision of section 4, articles 37 and following of the GDPR, WellCo project may not be obligated to designate a Data Protection Officer. The common project of WellCo could be considered exempt from the designation of DPO, while the processing of special categories of personal data, or the conducting of regular and systematic monitoring of data subjects is not realized on a large scale (article 37.1 GDPR). Nevertheless, **the recommendation of WP29 to designate a DPO, to give and ensure better compliance with the GDPR, even in the case that it is not required expressly by GDPR, should be taken into account.**

In addition, each partner of WellCo project must analyse the need of designation of DPO for their individual activity or for their consideration as public body or entities realizing activities for a public entity. At the time of this report, the DPOs have not been designated for the public authorities involved in the project.

However, once the GDPR is fully implemented, national regulation will be elaborated to define how the DPOs will be designated and when designated it will be communicated by the respective project partners to the WellCo Data Controller.

Phase	Measures
Phase 1	
Letter for participants Informed consent for participants Ethics Code for Professionals	Documents already elaborated and available in the project repository (Alfresco)
Phase 2	
Data controller designation	Designed as part of the DPIA procedure. Contract specifications for data controller in Appendix (Contract: Data Controller and Data Processor)
DPIA (Data Protection Impact Assessment) needed prior the processing of data	Guidelines for 3.2.5 - Data Protection Impact Assessment
Informed consent for participants	Informed consent for participants, in appendix.
Written agreement with mandatory provisions, whenever a data processor is engaged	Contract specifications for data processor in Appendix (Contract: Data Controller and Data Processor)
Designation of Data Protection Officer – each entity to assess the need of having a DPO	Document of designation of Data Protection Officer (DPO)

Table 10.- Data Protection Protocol Overview

APPENDIXES

Informed consent for participants

In_____on the__of__20__

INFORMATION ABOUT THE PROJECT

WellCo project is a research initiative funded by the European Commission (Horizon2020 programme, Grant Agreement No. 769765). The project is coordinated by Iberia Ingeniería y Proyectos S.L. (Spain) and has different entities involved (project partners) to ensure that the research aims are achieved. Three of these partners are responsible for gathering the necessary information and data to develop and test the proposed technologies, acting as pilot sites. In particular, the entities in charge of involving users and collecting their voluntary participation and data are:

1. Fondazione Bruno Kessler (FBK), Italy
2. University of Southern Denmark (SDU), Denmark
3. Gerencia de Servicios Sociales de Castilla y León (GSS), Spain.

These entities have specific collaborators, such as the University of Valladolid (in the case of GSS) and Cooperativa Kaleidoscopio (in case of FBK), which are involved as well in collecting data and/or end users information for the project purposes.

Once collected and after pseudonymisation, data will be processed by all project partners, which are, in addition to the already mentioned coordinator and pilot entities, the following: University of Copenhagen (UCPH, Denmark), Jožef Stefan Institute (JSI, Slovenia), Connected Care (CCare, The Netherlands) and Monsenso (Denmark).

The administration of the pseudonymised data will be centralised by the partner _____ (company name or name of the entity). In order to ensure that data collected and processed in the project are managed according to the regulation, a Data Controller will be designated.

INTRODUCTION/PURPOSE

WellCO aims at developing and validating radically new ICT based concepts and approaches for empowering and motivating people in need of guidance and care due to age related conditions, in cooperation with their carers where relevant, and to help them improve and maintain their independence, functional capacity, health status as well as preserving their physical, cognitive, mental and social well-being.

The "virtual coach" is going to provide personalised advice, guidance and follow-up for key age related issues in daily life which impact the person's ability to remain active and independent, for example diet, physical activity, risk avoidance, preventive measures, lifestyle and activity management, leisure, social participation and overall wellness.

The goal of WellCO is to preserve physical, cognitive, mental and social well-being for as long as possible and to facilitate interaction with carers (where relevant).

WellCO will guide seniors by offering personalised recommendations to motivate a behavioural change to a healthier lifestyle and to improve their quality of life, using the most innovative technologies, which can be carried out within their own social and geographical context and in coherence with their "Life Plan".

WellCO will involve end-users committed to help to design and develop the virtual coach as well as assess its user acceptability, satisfaction and impact in realistic settings.

TYPE OF RESEARCH

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

The research implies the collection of datasets from your wearable, your smartphone and via online surveys or questionnaires.

- Wearable. Two types of data will be collected from your device: aggregated data (e.g. step count/day, sleep types and times/day, heart rate/minute) and raw data (e.g. acceleration, orientation, raw activity, sleep, or heart data). You will only need to wear the device all day and night and charge it when needed. We will collect the device's datasets unobtrusively and in a secure and privacy-preserving manner.
- Smartphone. The following information will be collected automatically and unobtrusively from your phone in a secure and privacy-preserving manner: current time, location, signal strength, battery level, charging patterns, running applications, operator network status, WiFi and Bluetooth network status, screen brightness level/orientation, phone calls, SMS, amount of data sent and received on the network interface and lifestyle-related patterns. Content from phone calls, SMS or websites will not be collected, just the fact that you are using a particular application (e.g., browser/messaging application). No audio, video recordings will be made, only the logging of data on your smartphone.
- Surveys or questionnaires. Data on your personality traits, attitudes, lifestyle patterns, quality of life, etc. will be collected. Surveys may be provided onto the wearable, the smartphone, or other media. Security and privacy data collection and storage will be ensured.

PARTICIPANT SELECTION / VOLUNTARY PARTICIPATION

We have selected some people to participate in this innovative project; you are one of those selected and we hope to be able to count on you to achieve the objective to which we have committed.

You must be at least 18 years old to participate. If you choose not to participate in the study, you are free to do so at any time without any negative consequences.

DURATION

Your participation will take as long as you sign for, in any case no later than 30 of November 2020.

RISKS / BENEFITS / REIMBURSEMENTS

The risks and discomfort associated with participation in this study are no greater than those ordinarily encountered in daily life or while using a wearable, smartphone or tablet. The benefits, which may reasonably be expected to result from this study, are understanding of own lifestyle patterns and habits and to motivate a behavioural change in order to avoid risky health patterns and to improve or preserve your well-being and a better quality of life. We cannot and do not guarantee or promise that you will receive any benefits from this study.

CONFIDENTIALITY / SHARING RESULTS

All information collected on you as a participant and the acquired data are strictly confidential. The data will be used for research purposes only by the members of WellCo Project. The analysis results might be subject of scientific publications, always respecting the strict confidentiality or participants, so that any information will be anonymized prior to publication.

Each participant is assigned a code number. No information identifying the person is attached to the data; the data is pseudo-anonymized. Only the Data Controller (or designated data processor) keeps a list of the correspondence between the code and your identity (including your contact). This is necessary in order to contact you for a possible future use of the data

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

accordingly to article 13 GDPR. The experimenter and project managers are strictly bound by professional secrecy with regard to data and connections between data and subjects.

The data processing will finish on 30 November 2020 and all data will be deleted on 30 November 2025 at the latest.

All the data will be archived on our secure servers, with access protection and separate backup, under the responsibility of the Data Controller (or designated data processor). In addition, at your written request, your data can be erased at any time without any negative consequences to you.

We also inform you that the anonymized raw recordings, excluding any data that could lead to recognizing you, might be made accessible on an Open Science platform after the project end. This would allow sharing data with other researchers as a collaborative research tool.

RIGHTS OF DATA SUBJECT

If you have read this form and have decided to participate in this project, please understand your participation is voluntary and you have the right to withdraw consent or discontinue participation at any time without penalty or loss of benefits to which you are otherwise entitled. Note that the data provided during your participation in the study up to the moment of withdrawal can be used in the study.

- You have the right to access to and/or review your remarks in individual interviews and erase part or all of the recording or note, as well as you have the right to refuse to answer particular questions.
- You have the right to data portability on request.
- You have the right to lodge a complaint with supervisory authority.

CONTACT INFORMATION

If you have any questions, concerns or complaints about this study/research, its procedures, risks and benefits, of if you wish to opt-out from the study or make use of any other rights recognized by R(EU) 679/2016, please contact the Data Controller (or designated data processor): _____.

ENGAGEMENT OF THE PARTICIPANT

- ☐ I have read and understood all the information above.
- ☐ I accept to participate in the WellCo study/research.
- ☐ I authorise the entity _____ and the designated partners of WellCo Project to use my data for scientific purposes and that the results of the research aggregating my data and the data of other participants will be published in scientific journals or books. The data will remain confidential and no identity information will be given.
- ☐ I have voluntarily chosen to participate in this research. I have been informed that I may withdraw at any time without providing any justification and may, if necessary, request the destruction of my personal data. This consent does not relieve the organizers of the research of their responsibilities. I retain all my rights guaranteed by Nacional and European Regulation.

SIGNATURE AND DATE

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Document of designation of Data Protection Officer (DPO)

In _____ (place), to _____ (day, month, year)

_____ (Name and surnames), with Identification number _____, acting as _____ (position in the entity) of Entity _____ (company name or name of the entity) (hereinafter, the Entity), with ____ number, with sufficient powers for this act, and in compliance with REGULATIONS (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 2016, relative to the protection of natural persons in regarding the processing of personal data and the free circulation of these data and repealing Directive 95/46/EC (General Data Protection Regulation), I do the following,

DESIGNATION

_____ (Name and surname), as Data Protection Officer of _____ (company name or name of the entity).

This appointment implies the acceptance by the Data Protection Officer of each of the functions listed in the section "Functions and Obligations of the Data Protection Officer (DPO)" contained in the document of _____ (title indicate name of the internal regulations on data protection).

Likewise, the present appointment will have the objective of supervising and controlling compliance with the General Data Protection Regulations, as well as collaborating with the supervisory authority. In this sense, its validity will be understood for an indefinite period, and may be revoked by the General Management of the Entity at any time.

And in proof of compliance with the content of this document and for the appropriate purposes, I sign it in the place and date indicated.

_____ (Name and surname)

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Reply to the exercise of the right of opposition to the processing of personal data

_____ (Company name or name of the entity)

_____ (Name and surname)

_____ (Street, portal, floor, location)

In _____ (place), to _____ (day, month, year)

File No.: _____ (file number)

Dear _____ (surname):

In response to your letter dated _____ (day, month, year) in which we requested the opposition to the processing of your personal data in our files, we inform you:

That with date _____ (day, month, year) we have proceeded to make your right effective, in accordance with the following: The appropriate measures have been enabled to cease the processing of their personal data _____ (Indicate the data on which the right of opposition was exercised and on which the treatment has ceased), which were treated by our entity with the purpose of _____ (Determine the purpose that motivated the processing of data in relation to which the interested party has requested opposition to the treatment).

Additionally, we inform you that, since the right of opposition exercised by you implies the cessation of the processing of your data for the purposes of direct marketing developed by our entity, not only have the appropriate measures been authorized to cease the processing, but that in addition our entity has proceeded to the inclusion of your data in our Robinson List, ceasing to process your data for marketing purposes, Optional text as well as ceasing in the processing of their data for the elaboration of profiles related to the said marketing .

Inform you, also, of the existence of common general or sector exclusion files for the sending of commercial communications and, specifically _____ (Relate and identify those responsible for the common files, indicating their address and the data processing purposes).

Sincerely, Signed _____ (Name and surname)

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Reply to the exercise of the right of opposition to the processing of personal data

_____ (Company name or name of the entity)

_____ (Name and surname)

_____ (Street, portal, floor, location)

In _____ (place), to _____ (day, month, year)

File No.: _____ (file number)

Dear _____ (surname):

In response to your letter dated _____ (day, month, year) in which we requested the opposition to the processing of your personal data in our files, we inform you:

That it is not possible to grant such right due to:

Select one or another option

- ☐ There is a defect in the form that prevents the granting of the right and, in particular, the following:
- ☐ It has not been possible to verify your identity.

OR

- ☐ It has been exercised through a representative who has not provided sufficient supporting document.

Please correct the defect. As soon as our entity has proof of such correction and is in a position to grant the exercised right, we will proceed to make effective its right of opposition.

OR

- ☐ You have not clearly indicated in your request the personal data on which you wish to exercise your right of opposition. Please correct the defect. As soon as our entity has proof of such correction and is in a position to grant the exercised right, we will proceed to make effective its right of opposition.

OR

- ☐ There are a series of compelling legitimate reasons that prevail over the rights and freedoms that you assist, so that our entity continues to develop the processing of personal data on which you have exercised your right of opposition. Specifically, _____ (Determine the reasons that prevail over the rights and freedoms of the interested party and motivate the continuation of the treatment, as well as the legal basis thereof and the legal basis by which they prevail over the rights and freedoms of the interested party.)

OR

- ☐ The processing of personal data on which you have exercised your right of opposition is necessary for our entity, as it is necessary for the formulation (or exercise or defense) of claims. Specifically, _____ (Determine the legal basis that applies for the

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

denial of the right of opposition, based on the treatment with some of the indicated purposes that is being carried out in the entity.)

OR

- ☐ The personal data on which you have exercised your right of opposition are treated by our entity for the purposes of scientific or historical research (or for statistical purposes), such treatment being necessary for the fulfillment of a mission carried out by our entity. reasons of public interest. Specifically, _____ (Determine the legal basis that applies for the denial of the right of opposition based on the treatment with any of the indicated purposes being carried out by the entity, as well as the mission exercised by the entity for reasons of public interest that prevent the granting of the right of opposition.)

OR

- ☐ The personal data on which you have exercised your right of opposition are treated by our entity for the purposes of scientific or historical research (or for statistical purposes), such treatment being necessary for the fulfillment of a mission carried out by our entity. reasons of public interest. Specifically, _____ (Determine the legal basis that applies for the denial of the right of opposition based on the treatment with any of the indicated purposes being carried out by the entity, as well as the mission exercised by the entity for reasons of public interest that prevent the granting of the right of opposition.)

In any case, we inform you that you can exercise the rights of access, rectification, deletion, limitation of processing, portability of data or not being the subject of a decision based solely on automated processing, as well as withdrawing the consent given for the treatment of your data. Likewise, you have the right to file any type of claim with the pertinent Supervisory Authority, being in _____ the _____.

Sincerely,

Signed _____ (Name and surname)

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Reply to the exercise of the right to delete personal data ("right to be forgotten")

_____ (Company name or organization name)

_____ (Name and last name of the person in charge of the file)

_____ (street, portal, floor, location)

In _____ (place), to _____ (day, month, year)

File No.: _____ (file number)

Dear _____ (surname):

In response to your letter dated _____ (day, month year), in which you requested the deletion of your personal data contained in our files, we inform you:

That with date _____ (day, month, year) we have proceeded to delete in our File _____ (data of the file) the following data of its ownership:

_____ (Determine the suppressed data)

Additionally, we inform you that reasonable measures have been adopted by our entity to inform the following entities (or our entity has proceeded to inform the following entities) in relation to your request for suppression, in order that such entities have proof of said request and proceed, as far as possible, to the deletion of your data in any link, copy or replica of them that may be appropriate.

Sincerely,

Signed _____ (Name and surnames of the person in charge of the file)

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Reply to the exercise of the right to delete personal data ("right to be forgotten")

_____ (Company name or organization name)

_____ (Name and last name of the person in charge of the file)

_____ (street, portal, floor, location)

In _____ (place), to _____ (day, month, year)

File No.: _____ (file number)

Dear _____ (surname):

In response to your letter dated _____ (day, month year), in which you requested the deletion of your personal data contained in our files, we inform you:

- ☐ that it is not possible to grant such right due to: Select one or another option
- ☐ There is a defect in the form that prevents the granting of the right and, in particular, the following: Select one or another option
- ☐ It has not been possible to verify your identity.

OR

- ☐ It has been exercised through a representative who has not provided sufficient supporting document.

Please correct the defect. As soon as our entity has proof of such correction and is in a position to grant the exercised right, we will proceed to make effective its right of suppression.

OR

- ☐ You have not clearly indicated in your request the personal data on which you wish to exercise your right of withdrawal.

Please correct the defect. As soon as our entity has proof of such correction and is in a position to grant the exercised right, we will proceed to make effective its right of suppression.

OR

- ☐ The processing of personal data on which you have exercised your right of withdrawal is necessary to exercise the right to freedom of expression and information.

_____ (Determine the legal basis that applies to the denial of the right of withdrawal, based on the exercise of the right to freedom of expression or information that is being carried out by the entity through the processing of personal data about which abolished right)

OR

- ☐ The processing of personal data on which you have exercised your right of withdrawal is necessary for compliance with a legal obligation applicable to our entity, whose execution requires the processing of such data.

_____ (Determine the legal obligation applicable to the entity that prevents the granting of the right of withdrawal, as well as the Law / legal basis that imposes such obligation)

OR

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

- ☐ The processing of personal data on which you have exercised your right of withdrawal is necessary for the fulfilment by our entity of a mission performed in the public interest or in the exercise of the public powers that our entity has conferred, the execution of which requires of the treatment of such data.

_____ (Determine the mission exercised in the public interest applicable to the entity / task in exercise of public powers applicable to the entity that prevents the granting of the right of suppression)

- ☐ The processing of personal data on which you have exercised your right of withdrawal is necessary for our entity, for reasons of public interest in the field of public health.

_____ (Determine the specific reason why the granting of the right of withdrawal is not possible, based on reasons of public interest in the field of public health)

OR

- ☐ The processing of personal data on which you have exercised your right of withdrawal is necessary for our entity to be treating such data for purposes of archiving in the public interest (or for scientific or historical research purposes or for statistical purposes). In this context, the granting of the right of withdrawal by you exercised could make it impossible or seriously impede the achievement of the objectives of such treatment.

_____ (Determine the legal basis that applies for the denial of the right of withdrawal, based on the treatment with some of the indicated purposes that is being carried out in the entity)

OR

- ☐ The processing of personal data on which you have exercised your right of withdrawal is necessary for our entity, being necessary for the formulation (or exercise or defence) of claims.

_____ (Determine the legal basis that applies for the denial of the right of withdrawal, based on the treatment with some of the indicated purposes that is being carried out in the entity) In any case, we inform you that you can exercise the rights of access, rectification, limitation of treatment, opposition, portability of data or not being the subject of a decision based solely on automated processing, as well as withdrawing the consent given for the treatment of your data. Likewise, you have the right to file any type of claim with the pertinent Supervisory Authority, being in _____ the _____.

Sincerely,

Signed _____ (Name and surnames of the person in charge of the file)

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Reply to the exercise of the right to limit the processing of personal data

_____ (Company name or organization name)

_____ (Name and surname)

_____ (street, portal, floor, location)

In _____ (place), to _____ (day, month, year)

File No.: _____ (file number)

Dear _____ (surname):

In response to your letter dated _____ (day, month, year) in which we requested the limitation of the processing of your personal data in our files, we inform you:

That on date _____ (day, month, year) we have adopted the appropriate measures to limit the treatment that our entity performs such personal data. Specifically, the following measures have been adopted by our entity _____ (Determine the technical and organizational measures adopted to limit the data processing of the interested party)

During the time that this limitation of data processing lasts, we inform you that our entity could treat your personal data exclusively for any of the following purposes, and only in the case that the treatment is necessary for our entity:

- - For the fulfillment of the duties or data conservation needs that apply to our entity, in relation to the data whose treatment has been limited.
- - If you give us your consent for the treatment of your data whose treatment has been limited.
- - For the formulation, exercise or defense of claims.
- - To protect the rights of another natural or legal person.
- - For reasons of important public interest, imposed by the legal system of our country and / or of the European Union. Finally, we inform you that in the event that the limitation of data processing was lifted for any lawful reason, our entity will proceed to inform you properly before the lifting of said limitation.

Sincerely,

Signed _____ (Name and surname)

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Reply to the exercise of the right to limit the processing of personal data

_____ (Company name or organization name)

_____ (Name and surname)

_____ (street, portal, floor, location)

In _____ (place), to _____ (day, month, year)

File No.: _____ (file number)

Dear _____ (surname):

In response to your letter dated _____ (day, month, year) in which we requested the limitation of the processing of your personal data in our files, we inform you:

That it is not possible to grant such right due to:

Select one or another option

- ☐ There is a defect in the form that prevents the granting of the right and, in particular, the following:

Select one or another option

- ☐ It has not been possible to verify your identity.

OR

- ☐ It has been exercised through a representative who has not provided sufficient supporting document.

Please correct the defect. As soon as our entity has proof of such correction and is in a position to grant the right exercised, we will proceed to make effective its right to limitation of treatment.

OR

- ☐ You have not clearly indicated in your request the personal data on which you wish to exercise your right to limitation of treatment. Please correct the defect. As soon as our entity has proof of such correction and is in a position to grant the right exercised, we will proceed to make effective its right to limitation of treatment.

OR

- ☐ It has not been possible to determine the legal basis on which you base the exercise of your right to limit the processing of data, in accordance with the provisions of current legislation. Please correct the defect. As soon as our entity has proof of such correction and is in a position to grant the right exercised, we will proceed to make effective its right to limitation of treatment. Also, if you wish, you can contact our entity through the following email (or phone) _____ (indicate email or phone), in order to properly assess your request and determine the mode of attention of the same, the most efficient way possible.

In any case, we inform you that you can exercise the rights of access, rectification, deletion, opposition, to the portability of the data or not to be the subject of a decision based solely on the automated processing, as well as withdraw the consent given for the treatment of your

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

data. Likewise, you have the right to file any type of claim with the pertinent Supervisory Authority, being in _____ the _____.

Sincerely,

Signed _____(Name and surname)

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Reply to the exercise of the right to rectify personal data

_____ (Company name or organization name)

_____ (Name and surname of the person responsible for the file) _____ (Street, portal, floor, location)

In _____ (place), to _____ (day, month, year)

File No.: _____ (file number)

Dear _____ (surname):

In response to your letter dated _____ (day, month, year) in which you requested the rectification (or completion) of your personal data in our files, we inform you:

That with date _____ (day, month, year) we have proceeded to rectify (or complete) in our File _____ (type of file), the following data of its ownership:

_____ (Determine the rectified or completed data)

- ☐ That it is not possible to grant such right due to:

Select one or another option

- ☐ There is a defect in the form that prevents the granting of the right and, in particular, the following:

Select one or another option

- ☐ It has not been possible to verify your identity.

OR

- ☐ It has been exercised through a representative who has not provided sufficient supporting document. Please correct the defect. As soon as our entity has proof of such correction and is in a position to grant the right exercised, we will proceed to make effective its right of rectification.

OR

- ☐ You have not clearly indicated in your request the personal data to which it refers and / or the correction that must be made of them. Please correct the defect. As soon as our entity has proof of such correction and is in a position to grant the right exercised, we will proceed to make effective its right of rectification.

OR

- ☐ It is necessary that you accompany your request supporting documentation of the inaccuracy or incompleteness of your personal data, prior to the rectification (or completion) by our entity. Please correct the defect. As soon as our entity has proof of such correction and is in a position to grant the right exercised, we will proceed to make effective its right of rectification. In any case, we inform you that you can exercise the rights of access, deletion, limitation of treatment, opposition, portability of data or not to be the subject of a decision based solely on automated processing, as well as withdraw consent for treatment of your data. Likewise, you have the right to file any

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

type of claim with the pertinent Supervisory Authority, being in _____ the _____.

Sincerely,

Signed _____ (Name and surname)

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Reply to the exercise of the right to rectify personal data

_____ (Company name or organization name)

_____ (Name and surname of the person responsible for the file) _____
(Street, portal, floor, location)

In _____ (place), to _____ (day, month, year)

File No.: _____ (file number)

Dear _____ (surname):

In response to your letter dated _____ (day, month, year) in which you requested the rectification (or completion) of your personal data in our files, we inform you:

That with date _____ (day, month, year) we have proceeded to rectify (or complete) in our File _____ (type of file), the following data of its ownership:

_____ (Determine the rectified or completed data)

Optional text

Additionally, we inform you that your request for rectification (or completion) in relation to your personal data has been notified to the following entities, in order to rectify (or complete) your data in any link, copy or replica of the same that could be appropriate:

_____ (Company name or organization name)

Sincerely,

Signed _____ (Name and surname)

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Contract: Data Controller and Data Processor

In _____, to _____ of _____ of _____.

Mr./Mrs. _____.

And:

Mr/Mrs. _____

The parties involved recognized, reciprocal interest and sufficient legal capacity to subscribe this document, as well as to accept and assume the obligations established therein and, for that purpose,

Short Description of WellCO Project

- That by virtue of the above, the parties have agreed to the conclusion of this contract by _____ Data Controller/Responsible for the processing of data of WellCO Project enables _____ (Data Processor), to process the necessary personal data in the provision of the following service: _____

Or

- In the provision of their part of WellCO Project and with submission to the following:

CLAUSES

I. Definitions

Data Controller: natural or legal person, public or private nature, or administrative body, which decides on the purpose, content and use of the treatment.

Data processor: natural or legal person, public authority, service or other body that provides a service to the responsible party that involves the processing of personal data on his behalf. Unlike the person in charge who is the one who decides on the purpose and uses of the information, the person in charge of treatment must only comply with the instructions of the person entrusted with the provision of services.

II. Object

The main purpose of this agreement is:

- The processing of personal data required in the provision of WellCO Project according to the provisions of current regulations
- The specific tasks to perform are the following:

Optional text

- Data collection
- Data processing
- Specific tasks

III. Affected personal data or information

For the execution of the present contract _____ *(or company, entity or body),* data controller/responsible for the treatment, makes available to _____ (or company, entity or body), responsible for or part the treatment of personal data, the following information: Describe data information that will be provided

IV. Duration

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

This Agreement will have a duration of _____ (_____) *days (or months or years),* and will be extended for successive and equal periods, unless expressly stated in writing by any of the Members. This denunciation must take place at least _____ months before the end of the initial period of validity or any of its extensions.

In any case after the end of this contract, the person in charge of the treatment must return to the data controller (or any other person designated by the data controller) with all the personal data with which he has worked, as well as delete any copy of the same that is in his possession.

V. Obligations of the data processor

The person in charge of the data processing and all the personnel at your service is obliged to:

1. Use the personal data object of data processing, or those that it collects for its inclusion, only to fulfil the purpose of this assignment. In no case may you use the data for your own purposes.

2. Process the data according to the instructions of the data controller, informing him immediately in the cases of detection of any unlawfulness.

3. Record of all the categories of data processing activities carried out on behalf of the person in charge, which contains:

A general description of the technical and organizational security measures related to:

a. The pseudonymization and the encryption of personal data.
b. The guarantee of the confidentiality, integrity, availability and permanent resilience of the treatment systems and services.
c. The restoration of the availability and access to personal data quickly, in case of physical or technical incident.
d. Regular verification, evaluation and assessment of the effectiveness of technical and organizational measures to ensure the safety of treatment

4. Do not disseminate the data to third parties, unless you have the express authorization of the controller, in the legally admissible cases.

The data processor in charge can communicate the data to other data processors in charge of the treatment of the same data controller, according to the instructions of the data controller. In this case, the data controller will identify, in advance and in writing, the entity to which the data must be communicated, the data to be communicated and the security measures to be applied in order to proceed with the communication.

If the data processor must transfer personal data to a third country or to an international organization, by virtue of applicable Union or Member State law, he / she will inform the data controller for that legal requirement in advance, unless such right prohibits it. for reasons of public interest.

5. Subcontracting (1 of the 2 options)

Do not subcontract any of the services that are part of the object of this contract that involve the processing of personal data, except the auxiliary services necessary for the normal functioning of the services of the person in charge.

OR

Data processor is authorized to subcontract with the company _____ the services that entail the following data processes: _____

In order to subcontract with other companies, the data processor must communicate this in writing to the data controller, clearly and unambiguously identifying the subcontractor

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

company and their contact information. The subcontracting can be carried out if the data controller does not show his opposition within the period of _____.

The subcontractor, who also has the status of data processor, is also obliged to comply with the obligations established in this document for the data processor and the instructions issued by the data controller. It is the responsibility of the initial data processor to regulate the new relationship, so that the new data processor is subject to the same conditions (instructions, obligations, security measures ...) and with the same formal requirements as he, regarding the proper treatment of the personal data and the guarantee of the rights of the people affected. In the case of non-compliance by the sub-data processor, the initial data processor will remain fully responsible to the person responsible for compliance with the obligations.

6. Maintain the duty of secrecy with respect to personal data to which you have had access under this order, even after the end of its purpose.

7. Guarantee that the persons authorized to process personal data undertake, expressly and in writing, to respect confidentiality and to comply with the corresponding security measures, which must be properly informed.

8. Maintain at the disposition of the data controller the documentation proving compliance with the obligation established in the previous section.

9. Guarantee the necessary training of authorized persons to process personal data.

10. Assisting the controller in the response to the exercise of the rights of:

a. Access, rectification, deletion and opposition
b. Limitation of treatment
c. Data portability
d. Avoid being subject to automated individualized decisions (including profiling)

Execution (Select one or another option)

When the affected persons exercise the aforementioned rights, the data processor must communicate it by email to the address _____ (address indicated by the data controller) The communication must be made immediately and in no case beyond the following working day to the receipt of the request, together, where appropriate, with other information that may be relevant to resolve the request.

OR

The person in charge of the processing must resolve, on behalf of the person in charge, and within the established period, the requests to exercise the rights of access, rectification, suppression and opposition, limitation of the treatment, portability of data and not to be subject to individualized decisions automated, in relation to the data object of the order

11. Right to information (Select one or another option)

The data processor, at the moment of the data collection, must provide the information related to the data processing that will be carried out to data subjects. The wording and the format in which the information will be provided must be agreed with the data controller before the start of the data collection.

OR

It is the data controller's responsibility to provide the right to information to data subjects at the time of data collection.

12. Notification of data security violations

The data processor will notify the data controller, within the maximum term of 72 hours, and through _____, the violations of the security of the personal data (data breaches) under

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

his charge of which he has knowledge, together with all the information relevant for the documentation and communication of the incidence.

Notification will not be necessary when it is unlikely that such a breach of security constitutes a risk to the rights and freedoms of natural persons.

If it is available, at least the following information will be provided:

a. Description of the nature of the breach of the security of personal data, including, when possible, the categories and the approximate number of affected stakeholders, and the categories and approximate number of personal data records affected.
b. The name and contact details of the data protection delegate or other contact point where more information can be obtained.
c. Description of the possible consequences of the violation of the security of personal data.
d. Description of the measures adopted or proposed to remedy the violation of the security of personal data, including, if applicable, the measures adopted to mitigate the possible negative effects.

If it is not possible to provide the information simultaneously, the information will be provided gradually without undue delay.

13. Provide support to the data controller in carrying out the impact evaluations related to data protection, when appropriate.

14. Provide support to the data controller in carrying out the prior consultations with the supervisory authority, when appropriate.

15. Provide the data controller with all the information necessary to demonstrate compliance with its obligations, as well as to carry out audits or inspections carried out by the person in charge or by another auditor authorized by him.

16. Implement security measures:

In any case, you must implement mechanisms to:

a. Guarantee the permanent confidentiality, integrity, availability and resilience of the treatment systems and services.
b. Restore the availability and access to personal data quickly, in case of physical or technical incident.
c. To verify, evaluate and assess, on a regular basis, the effectiveness of the technical and organizational measures implemented to guarantee the safety of the treatment.
d. Pseudonymize and encrypt personal data, if applicable.

Destination of the data (Select one or another option)

Return to the data controller the personal data and, if applicable, the support media where they appear, once the service has been completed.

The return must involve the total deletion of the existing data in the computer equipment used by the data processor.

OR

Return to the data processor designated in writing by the data controller, the personal data and, if applicable, the support media where they appear, once the service has been completed.

The return must involve the total erasure of the existing data in the computer equipment used by the data processor.

OR

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Destroying the data, once the service has been completed. Once destroyed, the data processor must certify their destruction in writing and must deliver the certificate to the data controller.

However, the data processor can keep a copy, with the data duly protected or encrypted, as long as responsibilities for the execution of the present contract can be derived.

VII. Obligations of the data controller

Data controller shall:

a) Deliver to the data processor the data referred to in clause III of this document.
b) Carry out an evaluation of the impact on the protection of personal data of the treatment operations to be carried out by the person in charge if proceed or is required by GDPR.
c) Carry out the corresponding prior consultations if proceed or is required by GDPR.
d) Ensure, before and throughout the treatment, compliance with the GDPR by the data controller.
e) Supervise the treatment, including carrying out of inspections and audits if proceed or is required by GDPR.

VIII. Applicable Law and Jurisdiction

This contract will be governed and construed in accordance with GDPR (Regulation EU 2016/679 of the European Parliament and of the Council, of April 27, 2016) in what is not expressly regulated, subjecting the parties to the exclusive jurisdiction of the Courts and Tribunals of _____ for the resolution of any dispute that may arise between them with respect to the interpretation, validity, execution, compliance or resolution of this Agreement, with the express waiver of any other jurisdiction that may correspond to them.

And in proof and in accordance with all the foregoing, each of the Parties signs this Agreement in _____ (_____) copies, in the place and date indicated in the heading.

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Confidentiality and Professional Ethics Agreement

In_____ on the_____ of_____ 20_____

I, _____ with ID Card (tax identification number) _____ as professional belonging to the entity _____ linked to the development of the WellCo project, in accordance with my functions, and by virtue of the access to information relating to participating people and families, I agree to respect, in its integrity, the Organic Law 15/1999, of the 13th of December, on the Protection of Personal Data, the European Data Protection Regulation and other supplementary provisions, as well as their development standards.

Consistent with this,

1. I manifest that I am aware of my responsibilities in terms of not undermining the integrity, availability and confidentiality of the information that I will process. This information will be available only as regards the responsibility adquired by my institution within the consortium, as detailed in the proposal and the attached documment.
2. I agree to respect all ethical principles foreseen for preserving the privacy and dignity of all participants and persons involved. I agree to maintain professional secrecy with this regard over all personal data and any other sensitive information accessible by the entity _____ or myself during the project lifecycle.
3. I agree to respect the confidentiality of the actions carried out within the framework of the activities of this project. I will not modify and/or disclose any information or data obtained from said actions public, especially those relating to personal data, family, health, etc., maintaining the obligation of secrecy even after my relation with the parties concerned has finalised and, even, posterior to my employment relation with this entity.

As a consequence of the aforementioned, the information to which I have access, both regarding elderly persons and their families and next of kin, I will only share with the multidisciplinary team, with the professionals who form part of said team and, when necessary, by virtue of the tasks that are assigned within the framework of the project.

Signed _____ (Name and surname)

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Pre-Grant Requirements

In order to ensure that Pre-Grant Requirements are met in WellCo, the following sections explain how initial ethical issues regarding humans and protection of personal data will be addressed.

Requirement 2.1 – Details on the procedures and criteria that will be used to identify/recruit research participants.

As already mentioned, a minimum sample of 150 end-users composed by elderly people in need of guidance and care due to age related conditions, their relatives as well as multi-disciplinary experts will be involved since the very beginning till project end. These end-users will be placed in rural and urban areas of three different European geographical contexts and environments:

- Trento (Italy), users involved will be elderly (>65) living along in urban environments.
- Castilla y León (Spain), users involved will be elderly living alone (>65) in rural and isolated environments.
- Copenhagen area and the Southern Denmark area (Denmark), people involved will be early elderly (aged 55-65), in "good status" and in urban area.

Criteria

Criteria for defining the profile of the members of the sample, within the scope of each participating territory, will be established: Test trials with urban/rural environment and age group, according to each territory.

- a) In a rural environment (Castilla y León) it should be noted that the user for the test trials will be mostly:
  - Aged over 65,
  - Living alone (with informal caregivers in some cases),
  - With multiple pathologies and a certain level of fragility - mild (over 60 in Barthel Score/ Barthel ADL index), and
  - Able to follow independently healthy living guidelines: no cognitive impairment diagnosed: over 24 scoring in Mini–Mental State Examination (MMSE) or Folstein test.
- b) In an urban environment (Danish and Trento test trials), users will be:
  - Mostly age between 55 and 65 in Denmark and over 65 in Trento;
  - Healthy albeit with health-risk issues;
  - No cognitive impairment or associated dependency conditions as judged by the formal caregiver, e.g. GP or municipal health professional;
  - Recruited by the formal care-giver during clinical sessions.

Procedure

The recruitment of participants will be made from the databases of the territories performing test trials, in a purposive sampling, according to the previously defined criteria.

It will be tried, as far as possible, to achieve a gender paired sample.

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

The foreseen size of the sample would be increased at an agreed rate (around 10-15%) in order to reduce the mortality of the sample by reasons of abandonment and other adverse events.

The outlined procedure includes ordinary mail to the potential participant informing:

- His/her selection as a participant in the project;
- A summary of the information relating to the project drafted so as to ensure its understanding and motivate its participation;
- Selection procedure carried out;
- Main milestones of the project and the expected duration of their participation;
- Data relating to the appointment with their professional of reference, with the purpose of going into details of the project and to sign the informed consent regarding their participation.

In the Danish trial participants are also recruited from an intervention testing a model for prevention of chronic diseases (the TOF project). Participants will be verbally informed and handed a letter/leaflet, that provide the above information.

Requirement 2.2 – Detailed information on the informed consent procedures that will be implemented for the participation of humans.

Main explanation about the informed consent and the issues that it covers are shown in point 5 of this section.

The informed consent form will follow the national guidelines for informed consent and participant information for participation in clinical trials. Both the informed consent form and the participant information will be tested on the target population before trial commencement.

Informed consent will be part of the work process, assessment, and intervention with the participants.

Conformity must be managed through a personal interview with a professional in the social-health field who will guide and monitor the evolution of the person in the project. At that first meeting (after an official letter addressed to the selected person), the professional explains the content of the consent to the participant and his/her family caregiver, if available, before the documentation is signed.

Conformity must be managed through a personal interview with a professional in the social-health field who will guide and monitor the evolution of the person in the project. At that first meeting (after an official letter addressed to the selected person), the professional explains the content of the consent to the participant and his/her family caregiver, if available, before the documentation is signed.

Requirement 2.5 – Clarification of how consent/assent will be ensured in cases where adults may have cognitive difficulties and thus may be unable to give informed consent.

As mentioned in the user´s profiling, people with cognitive difficulties diagnosed will not be included in the target population address by this project.

Just in case there will be any participant with soft cognitive difficulties (e.g. some difficulties in understanding or writing-reading skills), the foreseen face-to-face interview will require the involvement of the family caregiver.

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765

Requirement 2.6 – Clarification of whether vulnerable individual/groups will be involved. Details must be provided about the measures taken to prevent the risk of enhancing vulnerability/stigmatisation of individuals/groups.

WellCo pilots will include elderly as target users and some of them may probably have a range of chronic disease. This aspect joined to the possible situation of loneliness, age and/or recent hospitalization, makes that they are them classified as vulnerable, or at least potentially vulnerable, because of their increasing risk of frailty. With the aim of assessing the features of this group as well as other possible vulnerable ones that pilots may involve, an study will be performed by the EUC, head of the EUEB, in D2.2 Ethics/gender and Data Protection Compliance Protocol.

Please note that a Common Informed Consent Form, according to the legislation in the different countries involved in the test trials, will be attached to the previous deliverable and provided to end-users. Those individuals who do not understand the nature, purpose and methodology of the study will be appropriately excluded from research. Anyway, taking into account the scope and objectives of the research, researchers should be inclusive in selecting participants. Researchers shall not exclude individuals from the opportunity to participate in pilots on the basis of attributes such as culture, language, religion, race, sexual orientation, ethnicity, linguistic proficiency, gender or age, unless there is a valid reason for the exclusion.

To reduce the risk of enhancing the vulnerability/stigmatisation of the above-mentioned individuals, a Letter of Commitment on Ethics will be signed in trials in Denmark (SDU), Italy (FBK) and Spain (GSS) as well as an Ethic Code for professionals, informal caregivers and volunteers. They, in turn, will be trained in strategies that promote good treatment and ethical behaviour towards vulnerable groups and avoid the performance of inappropriate or negligent behaviour, making a special impact in the detection of alarm signals that indicate the abuse of the rights of these groups. In addition, in the case of older people living alone, they will contribute to develop safe environments, by the elderly themselves or their caregivers, which are potentially harmful. These Good Clinical Practices will be supervised by the EUEB as well as the Ethical Committees created in every country participating in test trials.

Concern for the rights and wellbeing of end-users lies at the root of ethical review. The perception of subjects as vulnerable is likely to be influenced by diverse cultural preconceptions and so regulated differentially by localised legislation. It is likely to be one of the areas where researchers need extra vigilance. The EUC will ensure the fulfilment of the agreed Ethical Commitments for the WellCo Project, ensuring compliance with laws and customs, especially in these areas where vulnerabilities may not even be obvious until research is actually being conducted.

Security

Please, indicate if your project involves:

- ☐ Activities or results raising security issues: NO
- ☐ *EU Classified information* as background or results: NO

This project has received funding from *the European Union's Horizon 2020* Research and Innovation Programme under Grant Agreement No 769765