**eTryOn - Virtual try-ons of garments enabling novel human fashion interactions**

| | |
|---|---|
| **Project Title:** | **eTryOn - Virtual try-ons of garments enabling novel human fashion interactions** |
| **Contract No:** | 951908 - eTryOn |
| **Instrument:** | Innovation Action |
| **Thematic Priority:** | H2020 ICT-55-2020 |
| **Start of project:** | 1 October 2020 |
| **Duration:** | 24 months |

Deliverable No: D8.4

# Ethical, legal and privacy requirements and guidelines for implementation

| | |
|---|---|
| **Due date of deliverable:** | 31 January 2020 |
| **Actual submission date:** | 28 January 2020 |
| **Version:** | 0.3 |
| **Main Authors:** | Elisavet Chatzilari (CERTH) |

**Project funded by the European Community under the H2020 Programme for Research and Innovation.**

| | |
|---|---|
| **Deliverable title** | Ethical, legal and privacy requirements and guidelines for implementation |
| **Deliverable number** | D8.4 |
| **Deliverable version** | Final |
| **Contractual date of delivery** | 31 January 2020 |
| **Actual date of delivery** | 28 January 2021 |
| **Deliverable filename** | eTryOn_D8.4_final |
| **Type of deliverable** | Report |
| **Dissemination level** | PU |
| **Number of pages** | 37 |
| **Workpackage** | WP8 |
| **Task(s)** | T8.4 |
| **Partner responsible** | CERTH |
| **Author(s)** | Elisavet Chatzilari (CERTH) |
| **Editor** | Spiros Nikolopoulos (CERTH) |
| **Reviewer(s)** | Thomas De Wilde (QC) |

| | |
|---|---|
| **Abstract** | This deliverable will present the practices that will be followed by eTryOn in order to ensure that all ethical, legal and privacy requirements are adopted throughout both the implementation of the eTryOn technologies as well as the interaction with end users during the piloting phase. It will act as guidelines for the data collection and ownership processes both during the project pilots and research activities. |
| **Keywords** | Ethical requirements, privacy, data protection |

# Copyright

# Deliverable history

| Version | Date | Reason | Revised by |
|---|---|---|---|
| Alpha | 8/12/2020 | Table of Contents | Elisavet Chatzilari |
| Beta | 11/1/2021 | Beta version | Elisavet Chatzilari |
| Review | 21/1/2021 | Review comments | Thomas De Wilde |
| Final | 28/1/2021 | Final version | Elisavet Chatzilari |
| | | | |
| | | | |
| | | | |

# List of abbreviations and Acronyms

| Abbreviation | Meaning |
|---|---|
| AR | Augmented Reality |
| CFREU | Charter of Fundamental Rights of the European Union |
| CJEU | Court of Justice of the European Union |
| DPO | Data Protection Officer |
| EB | Ethics Board |
| EC | European Commission |
| ECHR | European Convention on Human Rights |
| EOPs | Equal Opportunities Policies |
| eIDAS | electronic IDentification, Authentication and trust Services |
| EU | European Union |
| GDPR | General Data Protection Regulation |
| HCI | Human-Computer Interaction |
| MR | Mixed Reality |
| PETs | Privacy Enhancing Technologies |
| PII | Personally Identifiable Information |
| PMB | Project Management Board |
| TFEU | Treaty on the Functioning of the European Union |
| UX | User Experience |
| VR | Virtual Reality |
| WHO | World Health Organization |
| WP | Work Package |

# Table of Contents

# List of Tables

# 1. Executive summary

This Deliverable (D8.4 - “Ethical, legal and privacy requirements and guidelines for implementation”) is the second deliverable for the Work Package 8 (“Management”). Its goal is to present all the necessary information regarding the human participation during the project and all the practices that eTryOn will follow in order to assure the data privacy, protection and confidentiality of the participants and their data generated throughout the project implementation and the pilots.

Firstly, the Ethics handling strategy is explained in Section 3. Specifically, any ethical issues that may arise, will be addressed with particular attention following established EU regulations and corresponding laws about user’s privacy, confidentiality and consent. In this section, one can also find all the applicable national, EU and international legislation, regulations and conventions around the Research on Humans.

Next, D8.4 presents all the details regarding the "Interaction with human participants" (Section 4). eTryOn refers to two categories of participants; Designers (pilot 1) and customers (who are going to use the public mobile applications for pilots 2 and 3). All of them will be provided with Information sheets and Consent Forms in order for the participants to be informed about the relevance and the content of the study as well as the protection of their personal rights, data management and privacy (Section 4.3).

The fact that eTryOn depends on participants’ data in a highly degree makes it essential to establish a strategy for their **data protection** (Section 5). The different data types (Questionnaires, body measurements, preferences on garments etc.) collected will be automatically anonymized or at least become pseudonymous. In all cases the personal identity of the user’s data will be strictly protected from third parties and will only be used for testing purposes within the project. eTryOn will comply with data protection acts, directives, and opinions, both at European and at National level (such as General Data Protection Regulation, Directive 95/46/EC, the Charter of Fundamental Rights of the EU, etc.). Moreover, eTryOn is going to comply with the various principles that have been introduced by Convention 108 and the Directive 95/46 (lawfulness, fairness, data minimization, storage limitation etc.) during the entire personal data lifecycle. eTryOn will apply all technical measures regarding the storage and transmission of the personal data. For instance, transmission of personal data over open communication channels will be done in encrypted form only. Finally, the eTryOn applications will follow a privacy-by-design methodology to ensure maximum protection of personal data.

Moreover, there is not any indicator that eTryOn will expose participants to physical harm during the project, since it will rely on the use of approved commercial VR glasses for the first pilot and commercial mobile devices for the other two pilots (Section 6). The deliverable ends by drawing some general conclusions (Section 7).

# 2. Introduction

In an era of significant breakthroughs in the fields of Artificial Intelligence (AI), Computer Vision (CV) and interactive technologies (e.g. VR, AR, MR), several sectors of the industry have benefited from these new technological achievements by embodying them in new innovative products: from self-driving cars to cashier-less supermarkets and from VR-enabled flight simulators for training air-force personnel to the more mainstream VR-based gaming. The fashion industry has been one of the industries that have been slow in incorporating these technological advancements in their business operations, in order to enhance both the creative process of garment design and the consumer interaction with fashion items. Indeed, the available interaction pathways have changed minimally over the past decades and mostly in the direction of encapsulating the recent social media frenzy (e.g. Instagram). With eTryOn, the use of interactive technologies will become mainstream in the fashion industry, focusing on three distinct fashion experiences that target both fashion designers and consumers: i) **creative experience**: while the creative process of garment design has changed over the past years from 2D sketches to using 3D design software, the visualization capabilities are still rather limited to just fitting the garments on grayscale predefined still avatars without considering the response of the garments during movements; ii) **social experience**: while the social experience of fashion has changed with the wide adoption of platforms like Instagram, it is still limited to just uploading images of people wearing physical clothes; and iii) **shopping experience:** the online shopping experience is essentially the same whether people buy clothes or electronics (i.e. they look at a few images of the items and their specs).

Building on recent advances in the fields of AI, CV and interactive devices, eTryOn's mission is to modernize the way people create, consume and experience fashion items (clothes) by offering novel Human-Fashion-Interaction (HFI) applications that i) enhance the creative process of garment design, ii) revolutionize the way people interact with fashion in the social media, and iii) simulate the physical in-store experience for online shopping.

The vertical innovation objectives of eTryOn that will transform HFI for the three interaction experiences mentioned above can be summarized as follows: a) generation of personal photorealistic 3D avatars of the user through a self-scanning application based on mainstream devices (i.e. smartphones), b) modeling of the interaction between the 3D photorealistic avatars and 3D garments (i.e. size fitting and visualization of interactions during movements) to provide improved realism, c) emerging fashion trend detection, user profiling and garment recommendations, and d) design and development of three novel HFI applications in VR/AR. Based on the results of the aforementioned innovation objectives, we propose to transform the current HFI experiences (i.e. creative, social and shopping), efficiently tackling the needs of both the consumers and the fashion industry.

Our objective is to design new interactive applications and devices that will be tailored to the end-users' needs (i.e. fashion designers and consumers). In this direction, our plan is to gather continuous feedback from the user base, starting from the beginning of the project (through collecting the user requirements) to its end (through iterative testing as well as through the envisaged pilots demonstrating the developed technology and the system update based on the users' evaluation). It goes without saying that a huge part of the project depends on participants' data. More specifically, during the project, three different applications will be piloted with actual users in order to test each one of the applications mentioned above. Therefore, for all the envisaged interactions with users, it is crucial to present all the necessary **ethical, privacy and legal related activities**, which will be performed prior to engaging with designers and consumers. In this direction, the objective of this deliverable is to review all the related legislative framework and present guidelines on how to manage all the project generated data assuring that all ethical, privacy and legal directives are followed by the project.

# 3. Ethics handling strategy

## 3.1 Ethics management

eTryOn will pay particular attention to any ethical issues that will arise and will address them in a professional way following established EU regulations and corresponding national laws about user privacy, confidentiality and consent. On that direction we have foreseen the eTryOn's Ethics Board in the organizational structure (see deliverable D8.1) of our project, which will be the responsible committee to depict and face all the rising issues that refer to ethics. In detail, the adopted ethical practices are described below.

The design and development of novel interfaces as well as the logging of the user's activity and learning progress, require careful deliberation of the ethical implications that may arise. eTryOn will have a strong focus on the **ethical assessment** of (i) the **impact of the data tracking infrastructure on the end users**, (ii) the **impact of the VR/MR applications and collaboration tool interfaces on the end users**, and (iii) the **design process** itself, with the intention of validating the approaches taken to address the fashion-related issues that the project is dealing with.

Appropriate methodologies for dealing with sensitive information and ensuring privacy will be applied at all stages of the data lifecycle, including the secure cloud-based storage of the data. Varying ethical policies of all countries involved and international regulations will also be taken into account. Members of the eTryOn consortium are well aware of European data protection legislations.

## 3.2 General ethics policy

All personal data that will become available during the project will be kept secure and unreachable by unauthorized entities. The data will be handled with appropriate confidentiality and technical security, as required by law in the individual countries and EU laws and recommendations.

A general policy on ethical conduct will be adopted by the eTryOn Consortium. Prior to the start of relevant eTryOn activities approval form responsible ethics committees will be requested in line with current regulations and guidelines and will explicitly address specifics related to the conduct of analyzing personal data, including procedures of (electronic or written) informed consent, remote data collection, user's feedback and privacy and confidentiality and cybersecurity in the data chain of the data and possible data sharing. The eTryOn activities will comply with all applicable national, EU and international legislation, regulations and conventions around the Research on Humans as depicted in the not exhaustive lists per topic below.

**Table 3.a: List of national, EU and international legislation, regulations and conventions around Research of Humans**

| | |
|---|---|
| **Human Rights** | • Universal Declaration of Human Rights (1948). Articles 12 and 29<br>• Universal Declaration on the human genome and human rights adopted by UNESCO (11-Nov-97) Declaration of Helsinki (WMA 2000)<br>• The Charter of Fundamental Rights of the EU (pending ratification of the Lisbon treaty)<br>• OHCHR: International Covenant on Civil and Political Rights, Article 7 (1976);<br>• WMA: Declaration of Helsinki (2004; http://www.wma.net/en/30publications/10policies/b3/);<br>• UNESCO: Universal Declaration on Bioethics and Human Rights (2005); |
| **Data protection & Confidentiality** | • General Data Protection Regulation (Regulation EU 2016/679)<br>• WMA Declaration of Taipei on Ethical Considerations Regarding Health<br>• eIDAS Regulation (EU 910/2014);<br>• Relevant ISO norms on data security and health data management such as ISO<br>• 27001 and ISO 27002.<br>• 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council (Safe harbour principle)<br>• Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.<br>• Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (Directive on privacy and electronic communications)<br>• Data Protection Directive 95/46/EC of the European Parliament and of the Council (1995),<br>• Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1985); |

# 4. Interaction with human participants

eTryOn will include human participants from various user groups, who will first define user requirements for the use case studies. These will be recruited by the end-user partners (ODLO, MLZ). End users will be recruited after obtaining their informed consent clearly stating that their responses will be used within eTryOn and only for research purposes (Section 4.3). The end-user partners will supervise their recruiting and evaluation procedure. The measurements and any other relevant content of the human participants will be anonymized for protection of the identities of the participants and compliance with EU and international regulations. Their de-identification will be based on two layers: scrambling of directly identifying information in structured data; free text parsing and tagging using dictionaries built with structured data to locate identifying data. Data de-identification will take place during the system evaluation in WP6.

Moreover, in the context of WP6 we will perform user studies and tests that include the interaction of humans with VR glasses and mobile applications. Following the best practice for ethics in Human-Computer Interaction (Ethics in HCI and Usability[1]), the data collected during the user evaluations will be automatically anonymized or at least become pseudonymous and used for research purposes only, not to be transmitted to third parties. In addition, any information given for community or personalization benefits will be given voluntarily. The data may include, but is not limited to, personal information about the user such as: name, date of birth, interests, scanning for clothes and, human bodies, location, preferences, images, or relations to other users. Even though the participation is voluntary and could even be anonymous, informed consent is necessary and will be sought from each individual user before her/his data is even stored. This will be accomplished by formulating acceptance terms of usage, and depending on how far-reaching data collection is, an informed consent will be requested at several levels of agreement (e.g. people may agree that eTryOn analyzes the data they create or upload on social media, but not their user interactions, because this may intrude deeper into their privacy).

## 4.1 Recruitment of human participants

For the eTryOn pilots, designers will be recruited from ODLO's fashion design team for the 1st pilot while mobile applications will become available to the public through MLZ's application. The marketing campaign of T7.2 will act as a recruitment campaign to attract pilot users.

## 4.2 Inclusion/exclusion criteria and non-discrimination practices

For the pilots of eTryOn we will only involve participants that are adults able to give informed consent, following the necessary procedures (Section 4.3). While our applications will be open to the public not discriminating on the users that can use them, we do not plan to involve vulnerable groups/individuals in a dedicated way, which eliminates the risk of stigmatization. Regarding gender-related aspects in the user involvement in the project pilots, men and women shall be involved in the same degree to the extent that is possible[2]. Great care shall be taken while collecting requirements, to implement these in such a way that all persons can work equally well with the proposed technology.

[1] Laurel, Brenda & Snyder, Carolyn & Quesenbery, Whitney & Wilson, Chauncey & Molich, Rolf. (2001). Ethics in HCI. 10.1145/634067.634197.

[2] http://ec.europa.eu/research/era/gender-equality-and-gender-mainstreaming_en.htm

## 4.3 Informed consent of the participants

The informed consent process is central to the ethical conduct of research. Appropriate informed consent from all participants will be obtained prior to inclusion into the eTryOn pilots. As it appears from the new guidelines on consent issued by the Article 29 Working Party, several elements are indispensable in reaching a valid consent[3]. First, consent should be freely given, which implies that the data subject is left with a real choice to consent. As such, it should not be bundled with non-negotiable terms and conditions nor involve detriment in case the data subject refuses to consent. Second, consent should be specific, i.e., given for a purpose well defined in advance. Third, consent must be informed and, therefore, be given after the data subject has received meaningful information about the controller identity, various purposes, types of data collected, existence of the rights granted to data subjects. All these details should be provided in clear and plain language whose wording matches the targeted audience. Finally, consent should reflect the data subject's unambiguous wishes by means of a clear affirmative act (e.g. unticked checkboxes). In eTryOn, account will be taken of all these elements when drafting and presenting a consent form. Furthermore, for each pilot case study, eTryOn will ensure that participants are aware of the right to withdraw from the experiments at any time, irrespective of whether incentives or other inducement have been offered for participation. In light of the experience of the trial or as a result of debriefing, the participant will have the right to withdraw retrospectively any consent given and to demand the destruction of their own personal data captured through the pilots. The refusal of a participant to participate or continue participating in the pilots will be always respected, while no pressure will be applied to the participants so as to ensure their participation. The participants will be withdrawn from the trials either through their own request, or through the advice of the pilot leader or Ethics Board. Upon withdrawal, all data collected from the participant will be instantly deleted. Subsequently, if necessary, the recruitment procedure will be re-initiated to select a replacement for the withdrawn participant.

In addition to classic processes, eTryOn aims to develop remote processes to obtain demonstrable participant consent as well. Participant Information Forms will be prepared according to data protection regulations. The information will be presented in a way to help the participants completely understand the relevant aspects of the study. Informed Consent and the ethical approvals will be submitted to the European Commission. An appropriate informed consent from participants has been and will be in place prior to use of their data. Informed consent will be prepared according to EU standards and written in a manner to enable laypersons to fully understand the aims of the studies, what the study procedures are, which information will be used and for what purpose. All potential participants will be informed about the relevance and the content of the study as well as about the protection of their personal rights, data management and privacy. Detailed information will be provided to the European Commission on the procedures that will be used for the participants' data (e.g. informed consent, direct/indirect incentives for participation, the risks and benefits for the participants etc.). In any case, consent will be obtained from all research participants included in the eTryOn.

We will make sure that the consents obtained from the participants will be:

a) **Informed**: given in possession and understanding of the principal, relevant information;

b) **Voluntary**: given freely and not as a result of coercive pressure (real or perceived);

c) **Competent**: given by somebody able, in virtue of their age, maturity and mental stability, of making a free, considered choice.

[3] Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (WP259).

In order to ensure the "**informed**" aspect, our research professionals will be proactive in providing accessible and non-technical information about the research to the participants, which is relevant to their decisions about whether or not to give access to their data (including the risks, benefits, alternatives and the nature and purpose of the research process). More specifically, we will ensure that the potential research participant is fully aware of, and fully understands: i) what the research is about; ii) why it is being conducted; iii) who it is being conducted for and who is funding it; iv) what the purpose of the study is and what will happen to the results; v) where the results will appear and who is likely to have access to them; vi) what will be expected of them if they agree to participate and how long their participation will take; vii) what anonymity and confidentiality mean in practice and make clear that the participant does not have to participate; viii) his/her right to withdraw from the research any time without detriment, even after having agreed to participate. Comprehension is essential and the professional needs to ensure that each participant understands what is involved in the eTryOn. This will be done in a manner that is clear to the people involved and in a manner that completely covers the information on the informed consent. In order to ensure the **voluntary** aspect, eTryOn will be sensitive to any available information about the individual situations of potential participants. Care will be taken so as to ensure that all participants are informed and that their choice about whether or not to participate is voluntary. The **competent** aspect will be ensured by asking the research participants to provide written consent (and/or physically agree in the Terms of Use). Thus, participants that are not able to give clear consent by signing the forms will do so by a person that was legally authorized to provide such consent on their behalf, or if the law of the country allows providing consent verbally. All consent forms, and alternative ways to provide informed consent, will be approved by the appointed ethical committees.

The three different pilots will take place with different end users. The first pilot will address fashion designers, the second pilot will target influencers and fashion lovers in general while the last will address fashion consumers and e-shoppers. For the designers, the informed consent will be comprised of two parts: a participant information sheet and a participant consent form. Within the participant information sheet, the following issues will be addressed where appropriate. The information will be provided in a question-answer format whereby technical and academic terms and jargon are replaced with plain language relevant to the stakeholder participating. Thus, the **participant information sheet** will include information as such:

- Project title
  - eTryOn - Virtual try-ons of garments enabling novel human fashion interactions
- Opening statement
  - Please will you take part in a study about…
- Why have you asked me to take part?
  - Basis of selection of participant
- What will I be required to do?
  - E.g. try out our garments virtually on your personal avatar, etc.
- Where will this take place?
  - The study will take place…
- How often will I have to take part, and for how long?
  - E.g. focus groups meetings, pilots
- When will I have the opportunity to discuss my participation?
  - Debriefing
- Who will be responsible for all the information when this study is over?
  - Inform the participants for the post-project procedure

- The destruction of all data collected and the information, when the project is over, is not needed for an official audit by the EU Commission
- Who will have access to it and for what reason?
  - Data related information
- What will happen to the information when this study is over?
  - Inform the participants for the data retention procedure
- How will you use what is found out?
  - Reports, publications, presentations
- Will anyone be able to connect me with what is recorded and reported?
  - Statement of confidentiality, details of coding system to protect identity
- How long is the whole study likely to last?
  - Details regarding the timeline of the project
- How can I find out about the result of the study?
  - Details regarding the results of the research
- What if I don't wish to take part?
  - Participation is totally voluntary
- What if I change my mind during the study?
  - Free to withdraw
- Do you have any other questions?
  - In that point, the designers will have the chance to ask anything which may be unclear to them regarding the study
- Details of who to contact with any concerns or if adverse effects occur after the study.

Once a participant has been given the time to read the information sheet and ask questions or raise any concerns, the participant will be given the consent form to sign which will detail their **informed consent** for taking part in the study. The **participant consent form** will include statements, for which the participants should fill the boxes if he/she agrees, such as:

**eTryOn Participant Consent Form for designers**

☐ I have read the Information Sheet for this study and all the details of the study have been explained to me.

☐ My questions about the study have been answered to my satisfaction and I understand that I may ask further questions at any point.

Regarding the second and the third pilots, since they aim at the general public, in terms of ethical requirements they are considered identical. For them, the participants will have to agree in the Terms of Use right before accessing the application. In summary, the Terms of Use will describe the **rights**, **obligations** and **restrictions** as well as provisions on **user protection** and **warranty disclaimers**. The provided rules address issues such as respecting the users' control and privacy, restrictions on content and use of the services, etc. With this approach, the specific implications (for example the conditions addressing data protection and privacy or copyright) will become clear. The Terms of Use may include, but not limited to, the following information:

**Table 4.a: Sample of the Term of Use for pilot 2 and 3**

| Title | Example |
|---|---|

| | |
|---|---|
| What these terms cover | This document sets out the terms of service for the use of eTryOn. To use our service, you must first have downloaded our app and accepted the end user license agreement which applies to the license of that app to you. If you do not agree to these terms, please refrain from using our app and service. |
| Why you should read them | Please read these terms carefully before using the app. These terms tell you who we are, what the project is about, how your data will be used, what to do if there is a problem, and other important information. If you think there is a mistake in these terms, please contact us to discuss. |
| Information about us and the project | Who we are, How to contact us, How we may contact you, etc. |
| Use of our service | To use our service, you must complete the registration process which you will be prompted to do once you have downloaded the app. Once you have registered for an account you will be able to use the services…,<br>This service is intended solely for users who are legally capable of forming a binding contract…,<br>We may restrict, suspend or terminate the account of any user who breaches these terms… |
| eTryOn's Obligations | Services, Compliance with Laws, Personnel and Performance, Documentation, Security Measures etc. |
| User's Obligations | User shall (a) comply with the eTryOn's acceptable Use Policy, (b) use the Services in accordance with the Agreement, etc. |
| Term and Termination | Participation is totally voluntary. Therefore, participants are aware of the right to withdraw from the experiments at any time, irrespective of whether incentives or other inducement have been offered for participation. |
| How we may use your data | Information for the scope of the project eTryOn and details regarding the research |
| Protection of User Personal Data | eTryOn will comply with data protection acts, directives, and opinions, both at European and at National level… |
| Subject's Rights | Participants have the right to access the data pertaining/related to them that is collected and processed in the context and for the purposes of the project. Participants have the right to request information, access, rectification, erasure (right to be forgotten) of their personal data or restriction of processing of personal data or to object to further processing as well as the right to lodge a complaint to the – competent- Data Protection Authority. |
| Limitation of Liability or Disclaimers | eTryOn shall use reasonable efforts to protect personal information submitted by you in connection with the eTryOn services and shall use such information in accordance with the privacy policy. |

| | |
|---|---|
| | You acknowledge and agree that your submission of any information is at your sole risk, and to the maximum amount permitted by law, eTryOn disclaims any and all liability to you for any loss or liability relating to such information in any way. |
| Entire Agreement | From time to time, we may implement additional terms and conditions applicable to specific areas or services of eTryOn or to particular content or transactions. These Terms of Use, the other documents referenced in these Terms of Use and such additional terms and conditions constitute the entire agreement between us and you regarding eTryOn and its content and services. They supersede and replace all prior agreements between you and us regarding the same subject matter. |
| Assignment | You may not assign or transfer these Terms of Use, by operation of law or otherwise, without our prior written consent. Any attempt to assign or transfer without our consent will be null and of no effect. We may freely assign this agreement. |
| Modifications | We reserve the right, at our discretion, to modify eTryOn and any services provided on it or to modify these Terms of Use, at any time and without prior notice. We will notify you of any material changes to these Terms of Use by posting the new Terms of Use and a redline of the changes on our website. By continuing to access or use eTryOn after we have posted a modification, you are indicating that you agree to be bound by the modified Terms of Use. If the modified Terms of Use are not acceptable to you, your only recourse is to cease visiting and using eTryOn. |
| Other important terms | Which laws apply to these terms and where you may bring legal processing |

Moreover, the Terms of Use may include some automated answers for the questions presented in the **eTryOn Participant Information sheet for designers** in order to inform the participants with more project-related information.

Once a participant reads the Terms of Use, he or she must physically check the following box to prove that they have read them, before using the eTryOn application.

**eTryOn Term of Use for consumers**

☐ **I confirm that I am over the age of 16 and I have read and agreed to the Terms of Use**

The above Consent and Information Forms (both for designers and customers) are just a sample. The final version of that will be updated and released in the following deliverables.

## 4.4 Ethical approvals guidelines

**Local and national ethics committees** – For all studies that involve humans, approval of the local and national ethics committees will be sought. A portfolio of all relevant documents such as ethical approvals, informed consent forms, information sheets, and policy documents concerning personal data, handling of incidental findings, transfer of data and material etc. will be compiled and submitted to the relevant research ethics committees for approval. If needed, raising issues will be discussed with the Ethics Advisor (WP8 – T8.4). Any ethical issues arising from these discussions will be taken up by the partners.

A sample of the informed consent/assent forms and information sheets is presented in this deliverable, while the final templates will be kept and submitted in future updated versions.

## 4.5 Data protection officer

The DPO of eTryOn (Ioannis Chalinidis from CERTH), whose contact details will be shared to all data subjects that will be involved in the research according to Article 13 of GDPR, will act as the data manager officer of the project to ensure that data processing actions within eTryOn are in line with the law. CERTH, as the beneficiary responsible for data management, will cooperate with technical and pilot partners to draft a detailed data management plan that will clearly identify how each dataset used or created by the project will be handled. CERTH will be responsible for closely monitoring the execution of the data management plan and ensuring that project partners handle project datasets appropriately.

# 5. Personal data protection

During the pilots of eTryOn (WP6), we will collect information about our participants that have to do with their profile, needs and abilities in what refers to their interaction with the virtual environments when carrying out the scenarios. In addition, the data may include, but is not limited to, personal information about the user such as: name, date of birth, interests, location or relations to other users. We only collect personally identifiable information if it is necessary for improving the user experience.

The concepts of 'controller' (Article 4(7) of the GDPR defines the controller as '*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*') and 'processor' (according to Article 4(8) GDPR, a **processor** is the '*natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*') play a **crucial role** in this part. Not only does the former allocate responsibility for compliance with data protection rules, but it also provides indications as to the applicable national law, the exercise of data subject's rights and the powers of national supervisory authorities.[4] On the other hand, the GDPR imposes specific rules on the latter in the context of confidentiality and security of the processing. Both these notions have been substantiated by the Working Party in a dedicated opinion[5]. In practice, the applications of these concepts to sophisticated situations involving numerous actors in the data processing chain have been proven more and more complex. However, qualifying the role of each player will be the very first step toward effective compliance. The data controller in our case will be CERTH and the data processor will be all the technical partners of the consortium (CERTH, QC, Metail and MLZ). In handling these data, we will make sure to comply with national and EU legislation, as well as follow the best practice for ethics in Human-Computer Interaction (Ethics in HCI and Usability).

## 5.1 Data protection directives

**Data protection** deals with '*personal data*', a notion defined by Article 2a of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and Article 4(1) GDPR as '*any information relating to an identified or identifiable natural person*'.

Although the qualification of the data at stake as 'personal' under the GDPR is paramount, attention should also be paid to the other elements circumscribing the applicability of the Regulation, whence the relevance of examining the GDPR's **material**, **personal** and **territorial** scope of application.

As stated in Article 2(1) GDPR, the Regulation applies to '*the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*'. Two notions therefore trigger the material applicability of the GDPR: the existence of a **processing** of **personal data**.

According to Article 4(2) GDPR, **processing** means '*any operation or set of operation which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,*

[4] See on that importance to qualify the various actors as soon as possible : Christina Tikkinen-Piri, Anna Rohunen and Jouni Markkula, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies' [2017] Computer Law & Security Review 8–9 <http://linkinghub.elsevier.com/retrieve/pii/S0267364917301966> accessed 10 July 2017.

[5] Article 29 Working Party, 'Opinion 1/2010 on the concepts of controller and processor' (WP169)

*dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*'. Basically, it encompasses everything that can be done with data, from their original collection to their definitive erasure. Given the functioning of the eTryOn project, there is no doubt that data will be collected, stored, pseudonymized, analyzed, aggregated, compared, visualized and used to extract relevant information to assist in the decisions regarding the implementation of the three pilots. In that sense, the intrinsic goal of the project is the 'processing' of data. Therefore, the first condition for the material application of the GDPR is very likely to be fulfilled.

For the processing of data to fall within the GDPR's scope of application, those must be 'personal'. **Article 4(1) GDPR** defines 'personal data' as '*any information relating to an identified or identifiable natural person ('data subject')*'. It further adds that '*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*'. However, it is of utmost importance, the Working Party recalls, that the scope of data protection rules is not overstretched at the risk of ending up applying data protection rules to situations which were not intended to be covered by those rules and for which they were not designed by the legislator. The opinion then suggests breaking this definition down in four building blocks, each of them being analyzed in detail below[6].

First, the notion of personal data encompasses '**any information**'. Now the Working Party does not define what 'information' is, but rather focuses on what kind of information would fall under the very wide notion of personal data.[7] As such, it recalls that, to be considered personal data, the *nature* of the information has no relevance. In other words, any kind of statement about a person, whether objective (*e.g.* the presence of a certain substance in one's blood) or subjective (*e.g.* behavior of a customer when dealing with a call center), true or not proven, may be considered as personal data. In the same vein, the *content* of the information does not matter, which means that the concept is not limited to information that refers to an individual's private and family life but also encompasses information on whatever types of activity are undertaken by him or her (*e.g.* information concerning a person's working relations or his/her economic and social behavior).[8] Finally, information may be considered as personal regardless of the *format or medium* in which that information is contained (*e.g.* data kept on paper or stored in a computer memory by mean of binary code or on videotape).[9] This very broad approach to information leaves, as noted by Purtova, the concept of personal data wide open to encompass vast amounts of data.[10] This has also been echoed in the Nowak case[11].

[6] For streamlined information on the notion of personal data under the GPDR, see *a.o.*: Eduardo Ustaran, *European Data Protection Law and Practice* (IAPP 2018) 60–64.

[7] For an in-depth analysis of the notion of 'information', see: Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' 8–12.

[8] Private and family life, home and communications/correspondence is, as explained in the previous section, rather the scope of application of the fundamental right to privacy as stated in Article 8 ECHR and Article 7 CFREU. This notion has also been interpreted very widely. See: ECtHR, *Amann v. Switzerland*, n. 27798/95, ECHR 2000-II, para. 65. In that sense, personal data might also fall under the scope of the right to privacy. It is, however, not necessarily the case.

[9] In that sense, Recital 15 GDPR underlines that '*the protection of natural persons should be technologically neutral and should not depend on the techniques used*'.

[10] As illustrated by Purtova (n 7) 10.

[11] CJEU, *Peter Nowak v. Data Protection Commissioner*, case C-434/16, para. 46.

Second, the information must '**relate to**' an individual. The Working Party considers that is the case when the information at stake is *about* that individual. In other words, one must assess the relationship between a specific piece of information and a person. In many instances, this link appears self-evident (*e.g.* employee's personal file kept by the HR department). In others, and when the information relates to objects, processes or events, this is not so striking (*e.g.* the value of a house which, while being about a material good rather than a person, still conveys meaningful information about its owner's wealth).[12]

Third, the information must relate to an '**identified or identifiable**' person. According to the Working Party, an individual is *identified* when, within a group of persons, he or she is distinguished from all other members of the group. On the other hand, *identifiable* means that, although the person has not been identified yet, it is possible to do so. The Working Party also differentiates between *directly* and *indirectly* identified or identifiable. While in the former case reference is made to a name (in combination with additional information if the name is not unique), the latter ties back to the so-called 'unique combination' phenomenon that allows the singling out of the person on the basis of multiple pieces of information, whether retained by the controller or not.

Finally, the information must relate to a '**natural person**'. In other words, personal data must be about living individuals. The cases of the *dead* and the *unborn* are therefore particularly interesting. The *former* are not covered by the notion of a natural person. This does not mean, however, that information relating to a dead person will always fall outside the definition of personal data. This would not be the case, for instance, when data about a deceased person also provides information on a living one (*e.g.* hereditary medical condition).

On the basis of Article 16(2) TFEU, the European Parliament, the European Commission and the European Council recently approved the **Regulation 2016/679** on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR)[13], which replaced **Directive 95/46**[14] as of the 25th of May 2018. The GDPR represents the core element of the so-called Data Protection Reform package, aiming at modernizing the legislative framework so as to allow both businesses and citizens to seize the opportunities of the Digital Single Market.

Crucial here is the **shift from a Directive** – which requires transposition into national legislation – **to a Regulation** – which is directly applicable in Member States' legal order.[15] In that sense, the Regulation clearly recalls that the still-into-force Directive 95/46 '*has not prevented fragmentation in the implementation of data protection across the Union*'. It then underlines that '*effective protection of personal data requires the strengthening and the setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data*'.[16] However, it should be noted that Member States still benefit from a wide margin of appreciation when it comes to

[12] In that specific context, the Working Party underlines that data protection rules wouldn't apply to such information when it is used solely to illustrate the level of real estate prices in a certain area.

[13] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] *O.J.E.U.*, L119/1. The Regulation will only apply as of the 25th of May 2018.

[14] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data [1995] *O.J.E.U.*, L281/31. This instrument will remain applicable until the 24 May 2018.

[15] See on that specific point and its implications: Henri De Waele, 'Implications of Replacing the Data Protection Directive with a Regulation - a Legal Perspective' (2016) 12 Privacy & Data Protection 3.

[16] Recitals 9 and 11 of the GDPR, respectively.

complement, particularize or even diverge from the rules laid down in the GDPR. This is for example the case for the age threshold governing child's consent, the exceptions to some of the data subject's rights, the provisions dealing with the data protection officer and the rules on transfers.[17] However, the core principles remain pristine. All in all, the GDPR reinforces the regulatory framework introduced by the Directive. While relying on the same concepts and definitions, it complements them with welcome additions and expands the previous regime with regard to its territorial scope, the responsibilities and obligations of the controllers and processors and the powers and duties of the national supervisory authorities. Among other novelties, it now introduces a risk-based and accountability approach allowing controllers to tailor the extent of their compliance duty to the threats caused by their processing activities.[18] Finally, the enforcement of the rules has been paired with drastically increased administrative fines, new criminal penalties and more effective judicial remedies.

Regarding eTryOn's data protection strategy, any data collected for user or context modelling will be strictly anonymous. In all cases the personal identity of the data will be strictly protected from third parties and will only be used for testing purposes within the project. eTryOn will comply with data protection acts, directives, and opinions, both at European and at National level.

These include:

- The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). The primary objectives of the GDPR are to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
- Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- The Charter of Fundamental Rights of the EU, specifically the article concerning the protection of personal data.
- The opinions of the European Group on Ethics in Science and New Technologies in their report "Citizens Rights and New Technologies: A European Challenge" on the Charter on Fundamental Rights related to technological innovation.
- In particular recommendations related to ICT concerning data protection and individual's freedom and autonomy.

As far as the data becoming available to the consortium by external sources, formal consent is also necessary and will be sought from the data owner before this data becomes part of eTryOn's platform. The research in eTryOn will involve the collection of "Personal Data" including "Sensitive Data", in line with the new **General Data Protection Regulation (GDPR)**.

[17] On that point, see Winfried Veil's map on the opening clauses in the GDPR <https://www.flickr.com/photos/winfried-veil/24134840885/in/dateposted> accessed 1 November 2017.

[18] Stefano Varotto and James Colin, 'The European General Data Protection Regulation and Its Potential Impact on Businesses: Some Critical Notes on the Strengthened Regime of Accountability and the New Sanctions' (2015) 20 Communication Law 78.

In any case, GDPR will play a significant role by providing a legal basis on which grounding the processing of one's personal data and establishing balancing mechanisms whose implementation are left up to controllers. Ultimately, one should recall that the GDPR aims at protecting data subjects' fundamental rights with regard to the processing of their personal data and, as such, acts as an enabling instrument aiming for the overall respect of these rights and freedoms[19].

## 5.2 Types of data collected by eTryOn

All of the data collected and processed within eTryOn is relevant and limited to the purposes of the research project (in accordance with the 'data minimization' principle). Follows from Art. 5(1)c GDPR. This essentially calls for a necessity and a proportionality test. When it comes to the former, controllers should make sure that they only process personal data that are suitable and reasonable to accomplish the purposes specified according to the purpose limitation principle. In other words, controllers should assess whether these purposes could be achieved with either less data or with properly anonymised data sets. As to the latter, it requires controllers to tailor the amount of data collected, as well as their retention period, to the identified purposes.

Therefore, the following data will be collected during eTryOn and for the following reasons:

- Demographic details including: age, gender, etc. (WP3, WP6)
- Preferences on garments and designs for user profiling and proving the users with garment recommendations (WP3)
- Data from questionnaires for gathering requirements in the eTryOn design and evaluating the applications (WP6)
- User body measurements and visual data (i.e. scanning of faces/bodies for photorealistic avatars) will be used for creating photorealistic personal avatars (WP1) and fitting garments on them (WP2), while the user will have full control over them through the eTryOn applications (WP5).

Sensitive personal data will not be collected during eTryOn (by sensitive the following types of data are considered; personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation).

The use of other types of data is also dependent on the design of the eTryOn. Relevant policies will be adopted if for example more personal information is collected (e.g., the purpose for which access to the data is requested, whether secondary analysis of data will be performed). Data consumers will be allowed to use the data for performing the desired application features (e.g. fitting, getting garment recommendations) provided from the eTryOn applications. During the architecture design process of eTryOn (D4.1 to be delivered in M8), a privacy-by-design methodology will be adopted in order to ensure the secure storage and access of the data as well as their protection.

## 5.3 Data collection storage, transmission and security principles

In order to be aligned with EU data privacy laws and regulations, within WP8 appropriate privacy-preserving mechanisms dealing with sensitive personal information will be applied

[19] See on that point Rec. 4 GDPR: '*This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity*'. Therefore the GDPR does not solely enable privacy and data protection.

to ensure data privacy and prevent privacy-related leakages when collecting and processing personal data (T8.4). The Ethical Advisory Board will be consulted throughout the project and relevant reports will be submitted to ensure compliance with each country's ethical standards, as well as the latest European legislation.

In eTryOn, the appropriate data interfaces for enabling integration with existing data repositories will be implemented. On top of these, appropriate mechanisms will be developed to ensure data privacy and users' de- identification when querying databases or sharing anonymized records. In order to tackle the ethical issues deriving from the whole WP8, the eTryOn consortium will reinforce the proposed solution with means of data anonymization and de-identification that will take place in WP8 (T8.4) "Ethical, legal and privacy requirements and guidelines for implementation". Additively, the eTryOn consortium will establish a legal, ethical and privacy framework and Data Protection Framework dealing with the privacy protection and security for accessing and communication of personal data while verifying compliance of services to European legislation (e.g. General Data Protection Regulation (EU 2016/679) and EC Directive 46/95 on data protection) and to the corresponding specific national legislation. It should be noted that the consortium will follow the latest developments concerning the protection of individuals with regard to the processing of personal data and on the free movement of such data. Therefore, anonymization is crucial not only for coordination of data analyses across researchers, but also so that data preparation meets the guidelines binding different researchers and authorities. To support secondary analysis, eTryOn will develop an EU-compliant data protection framework in order to efficiently tackle privacy and data protection issues in data analytics and simulation activities. This framework will guarantee users' high standards of data and privacy protection and will foresee specific rules for sharing and reusing heterogeneous data between participants, data providers and researchers.

The project is designed to support the secure transport of information between consortium members – data providers, and this gives rise to scenarios in which the ethical handling of personal data will be required. Each of these is examined below and the implications for ensuring ethical treatment within a framework of information governance are considered. Therefore, inspired by the EC Co-ordination Action 'STEP' (FP6 IST-027642), which presents a survey of legal and ethical issues for the Virtual Physiological Community, we examine the same checklist of the STEP findings for eTryOn:

**Table 5.a: Survey of legal and ethical issues for the Virtual Physiological Community**

| Topic | Description | eTryOn |
|---|---|---|
| Informed consent for research | As a fundamental principle, individuals should be fully informed about the use to which their data will be put, and the protocols under which it will be collected and handled. Consent should be obtained before use in all cases. | Fully compliant. Data used during the project will be fully consented |
| Privacy, protection data | All data collected from humans, whether ab initio or from existing databases, must comply with the requirements of applicable data protection law. | Fully compliant. All partners conform to applicable data protection regulations |

| | | |
|---|---|---|
| Duty to inform, and the right 'not to know' | Research subjects may prefer not to know incidental findings from research projects, and there are ethical issues concerning the transfer of untested findings to subjects generally unable to assess their quality | Not applicable. No medical research findings to communicate |

### 5.3.1 General Principles for handling and protection of human data in eTryOn

In order to ensure safety, the available data will be automatically anonymized or at least become pseudonymous and will not be transmitted to third parties. Article 4(5) GDPR defines **pseudonymization** as '*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*'. eTryOn will investigate the latest anonymization techniques in order to utilize the most appropriate ones, while data quality estimation will also be performed to guarantee the consistency and reliability of the information. Only data that are of relevance for the proposed research will be collected, no excess data will be stored. Data will only be processed for eTryOn research purposes.

Moreover, the protection of personal data will also be ensured through procedures and appropriate technologies, like the use of HTTPS protocol for the encryption of all internet transactions and appropriate European and Internet security standards from ISO, ITU, W3C, IETF and ETSI. To assure participant's privacy, all data will be anonymized, encrypted and stored on a server to which only the relevant staff have access. More specifically the server onto which the data will be stored will have server-side encryption. That means that the server's administration personnel will be able to generate public keys for specific personnel who will have access to the data but will not be able to access the data themselves (since the private keys required for this access will be generated on the machine of the person with access to the data). This means that only the required personnel will have access to the data and even in the remote case of a possible data leak or server hack the data stolen will be fully encrypted and thus fully non-accessible.

In general, the GDPR fine-tunes, complements and explicitly names the **various principles** that were already introduced by the Convention 108 and the Directive 95/46, namely (a) lawfulness, fairness and transparency, (b) purpose limitation, (c) data minimization, (d) accuracy, (e) storage limitation, (f) integrity and confidentiality and (g) accountability. For that reason, personal data collected in eTryOn will be processed in compliance with relevant legislation and guidance, and applicable international, EU and national law, specifically the General Data Protection Regulation No 2016/679 and ISO norms 27001, ISO 27002, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995) and national legislation, which includes:

In general terms the appropriate data protection principles will be observed, including:

- Data are fairly and lawfully processed;
- Data are used only in ways that are compatible with the original consent;
- The amount of data collected is relevant and not excessive;
- All reasonable efforts are taken to ensure data accuracy;
- The data are used in accordance with the rights of the study participant;
- The data are stored securely;
- The relevant international and national guidance will be followed.

- Compliance with the original study consent for which data were collected;
- Personally Identifiable Information (PII) is adequately protected;
- Ensure that anonymization/de-identification is conducted appropriately;
- Ethical review is completed as required;

Moreover, special procedures will be developed on how participants can log in and give consent according to at least the assurance level 'substantial' according to the eIDAS Regulation and how a trial ID (pseudonym) of the participant can be generated under which data and possible samples will be collected and transferred to the eTryOn database. Special attention will be given to the cyber security issues and especially when that involves the use of mobile devices. Proposals for data handling during the project will be presented to the independent ethics advisor for ethical assessment. Data management and data sharing is a key issue in the eTryOn project. Data handling is based on the Guidelines for Data Management in the Horizon 2020 program. We will devise a data management plan which will give detailed information on procedures which can be implemented for data collection, storage, disclosure, protection, verification, modification, transfer and deletion in eTryOn by the consortium. It will give details on how the research and organizational data of the consortium will be stored, handled, shared and protected.

### 5.3.2 Privacy, confidentiality, anonymity and security

Privacy and data protection (discussed in the previous sections) are often confused and the relation between these two rights is considered to be complicated. Hence, the necessity to highlight the similarities and differences between these two notions before delving into the relevant regulatory frameworks.

Regarding their similarities, Privacy and data protection are both **fundamental rights**. While the former is protected under Article 8 of the European Convention on Human Rights (ECHR)[20] and Article 7 of the Charter of Fundamental Rights of the European Union (CFREU)[21], the latter has no direct counterpart in the ECHR but is enshrined in Article 8 of the CFREU. Two systems therefore ensure the protection of privacy and data protection in Europe[22].

Any interference with a fundamental right requires justification. This implies answering a twofold question: 1) is there any interference with one's right to privacy or data protection and, in case there is, 2) is the interference justified. As far as the **first question** is concerned, the ECtHR has already acknowledged that the collection, storage or disclosure of information relating to private life interferes with the right to privacy.[23] On the other hand, the CJEU has stated that, in establishing the existence of an interference with the fundamental right to respect for private life, '*it does not matter whether the information is sensitive or whether the person concerned have been inconvenienced in any way*'.[24] In other words, the processing of data about individuals is likely to interfere with their right to privacy and data protection and, as such, might require justification. When it comes to permissible interferences with the right to data protection, Article 8(2) CFREU adds an important precision: data must be processed '*fairly for specified purposes and on the basis*

[20] Council of Europe, Convention for the Protection of Human Rights and fundamental Freedoms, signed in Rome, 4 November 1950.
[21] Charter of Fundamental Rights of the European Union, *O.J.E.U.*, 18 December 2000, C 364/01.
[22] Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222, 222.

[23] ECtHR, *Amann v. Switzerland*, n. 27798/95, ECHR 2000-II, para. 65, 69, 80; ECtHR, *Rotaru v. Romania*, n. 28341/95, ECHR 2000-V, para. 46; ECtHR, *Leander v. Sweden*, n. 9248/81, para. 48.
[24] CJEU, *Österreichischer Rundfunk and Others*, case C-465/00, C-138/01 and C-139/01, para. 75; CJEU, *Digital Rights Ireland*, joined cases C-293/12 and C-594/12, para. 33.

*of the consent of the person concerned or some other legitimate basis laid down by law*'. In such cases, there is no interference with the right to data protection.[25] However, the collection, use and storage of these data might still interfere with the right to privacy and therefore require justification under Article 8 ECHR and 7 CFREU.[26]

Regarding the **second question**, Article 8(2) ECHR and Article 52(1) CFREU detail the conditions under which an interference with the right to privacy and data protection may be justified. According to these provisions – that introduce the so-called three-step test – any interference with the fundamental rights guaranteed must 1) be in accordance with the law, 2) pursue one or more of the exhaustively cited legitimate interests and, finally, 3) be necessary in a democratic society.[27] Additionally, Article 52(1) recalls the general principle of proportionality, which requires that '*the content and form of Union action shall not exceed what is necessary to achieve the objectives of the treaties*'.[28]

Privacy and data protection do, however, differ by their scope. As it appears from Article 8 ECHR and Article 7 CFREU, **privacy** is concerned with '*private and family life, home and correspondence/communications*'.[29] On the other hand, **data protection,** as discussed in the previous section**,** deals with '*personal data*', a notion defined by Article 2a of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and Article 4(1) GDPR as '*any information relating to an identified or identifiable natural person*'. Although these concepts appear similar, they don't always overlap.

**Table 5.b: Privacy and data protection from a Fundamental Right perspective**

| | | Privacy | Data Protection |
|---|---|---|---|
| **Legal basis** | Council of Europe | Art. 8 ECHR | Art. 8 ECHR (derivative) Convention 108 |
| | EU | Art. 7 CFREU | Art. 8 CFREU |
| **Scope** | Council of Europe | Private and family life, home and correspondence | Personal data |

[25] CJEU, *Volker und Markus Schecke and Eifert*, joined cases C-92/09 and C-93/09, para. 49
[26] Kokott and Sobotta (n 23) 226.

[27] These conditions stem from Art. 8(2) ECHR. Art. 52(1) CFREU, while being phrased differently, prescribe a very similar test. As such, '*any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*'.
[28] Art. 5(3) of the Treaty establishing the European Union, *O.J.U.E.*, 26 October 2012, C326, pp.13-390. See also these cases on the proportionality requirement: CJEU, *Afton Chemical*, case C-343/09, para. 45; CJEU, *Volker und Markus Schecke and Eifert*, joined cases C-92/09 and C-93/09, para. 74; CJEU, *Nelson and Others*, joined case C-581/10 and C-626/10, para. 71; CJEU, *Sky Österreich*, case C-283-11, para. 50; CJEU, *Schaible*, case C-101/12, para. 29.
[29] European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights' <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 14 March 2018.

| | | | |
|---|---|---|---|
| | EU | Private and family life, home and communications | Personal data |
| **Interference** | Council of Europe | Justification under Art. 8(2) ECHR | Justification under Art. 8(2) ECHR (derivative) |
| | EU | Justification under Art. 52(1) CFREU | No interference if conditions of Art. 8(2) CFREU are met<br>Justification under Art. 52(1) CFREU |

To deal with the ethical issues about personal data that may arise, the eTryOn consortium will take into consideration the Code of Conduct for User Experience (UX) Professionals[30] and especially paragraph 6, according to which, privacy, confidentiality and anonymity shall be respected in any relevant study. Paragraph 6 states that:

- UX practitioners shall not reveal information that identifies colleagues or participants without their permission and shall take reasonable precautions to avoid such information from being disclosed unintentionally;
- UX practitioners shall ensure that participants in any study provide informed consent for use of all data collected;
- UX practitioners shall never disclose in their writings, reports, teaching materials or other public media or otherwise make public any information they have acquired about persons, employers or clients in the course of their professional work unless disclosure is both legal and that they have either taken reasonable steps to disguise the identity of the person, employer or client, or they have the express permission to disclose.

In this direction, relevant data protection measures will be taken so that the security of the data is guaranteed. The consortium's main priority will be to ensure respect for the persons behind the data and consideration of the potential harm to individuals or communities. Information in excess of the strictly required data will not be employed, in order to avoid gathering data that is irrelevant. Quality of data will be taken into account and specific measures will be adopted to ensure that the data provided by the participants is up to date and accurate, including providing adequate information to the participants and maximum transparency. Within the consortium, members will take individual responsibility and hold each other accountable for the criteria use to make decisions.

In order to ensure that the anonymity of the participants is kept, technical and organizational measures will be taken to ensure that the personal data are not attributes to an identified or identifiable natural person. In this direction, all the data that could be used to identify the participant will be kept locally at their device, while there will be pseudonymization techniques in place that properly protect user's identity. Pseudonymization is a branch of anonymization. The key differentiator with pseudonymization is that it substitutes attributes with other values so that the original data can be reconstructed with additional information. Pseudonymization can be considered as a form of coding (the process of converting symbols in a message into another encoded set of symbols). This technique is useful where attributes in a dataset need to be uniquely identified but their actual value does not need to be kept. When applied, the values used to replace original values should not be derived in any way from the original values.

[30] http://uxpa.org/wp-content/uploads/2018/08/CoC_English.pdf

In order to make the process reversible, the database storing information required to facilitate the reversal should be kept to separate and secure from the pseudonymized dataset.

### 5.3.3 Data subject's rights

The shift from the Directive 95/46 to the GDPR was a timely opportunity to **strengthen the various data subject's rights** and, more specifically, to harmonize the practical modalities governing their exercise. In that sense, the move to a Regulation mirrors the EU institutions' wish to build a '*strong and more coherent data protection framework given the importance of creating the trust that will allow the digital economy to develop across the internal market*' (Recital 7 GDPR). Recalling that the Directive 95/46 '*has not prevented fragmentation in the implementation of data protection across the Union*', the Regulation underlines that an '*effective protection of personal data requires the strengthening and the setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data*' (Recitals 9 and 11 GDPR, respectively). To this end, it pairs the rights of data subjects with clear-cut modalities, clarifies the rights that were already laid down in the Directive 95/46 and introduces a new right of data portability. Given that the objective of this deliverable is not to provide an extensive review of all these prerogatives, only a summary of them is presented in Table 5.e. Finally, considering that within eTryOn data processing is not expected to result in a high risk to the rights and freedoms of data subjects, a Data Protection Impact Assessment is not required.

**Table 5.e: Data subject's rights**

| Name | Article | Subject's Right |
|---|---|---|
| Modalities | 12 GDPR | Among other, any communication issued by the controller in that context must be phrased in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Article 12(1) GDPR). |
| Access to the data | 15 GDPR | Grants the data subject the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where this is the case, **access** to these data |
| Right to rectification | 16 GDPR | Allows the data subject to obtain from the controller the rectification of inaccurate personal data concerning him or her without undue delay. |
| Right to erasure | 17 GDPR | This prerogative allows data subjects to seek erasure of their personal data in specific cases |
| Restrict the processing | 18 GDPR | The controller may keep the personal data at stake, but must refrain from using them during the period for which the right applies |
| Right to data portability | 20 GDPR | This newcomer allows data subjects to receive their personal data in a structured, commonly used and machine-readable format and to transmit them to another controller without hindrance from the original controller in specific cases |
| Object | 21 GDPR | Offers the data subject the possibility to object, on grounds relating to his or her particular situation, to the processing of their personal data in specific cases |

| | | |
|---|---|---|
| Right not to be a subject | 22 GDPR | Right not to be subject to a decision based solely on automated processing which produces legal effects concerning him or her or significantly affects him or her.[31] |

### 5.3.4 Storage and transmission

eTryOn will observe European legal regulations concerning privacy. This is at a policy level, and will be monitored and reinforced by eTryOn Coordinators, Boards and the CERTH legal department. At the technical level reasonable technical measures concerning data security of personal and sensory data will be applied. For instance transmission of personal data over open communication channels will be done in encrypted form only. The partners have considerable experience with such privacy protection measures, either because it belongs to their core business, or because they have collected corresponding experiences in related projects.

**Retention**: Three months after the project completion all personal data that have been collected, stored and processed will be deleted. If there is a need to further process the data after the end of the project, the researcher will have to obtain a new consent from the participants.

**Usage**: eTryOn will further comply with Article 8 of the European Human Rights Convention. All pilots involving under aged and adult participants will be performed by qualified staff and with the practical experience, which will guarantee a strict conformance with national and international ethics and regulations. The consortium is committed to maintain strict rules of privacy and prevent all personal data from being abused or leaked. The collected data will be used strictly for the purposes defined by the project objectives. Under no circumstances, the consortium will provide, give or sell any information of its users to any third party (data will not be used under any circumstances for commercial purposes). Central to this framework are principles concerned:

1. recognizing the primacy of the views, choices of users and respect of their dignity;
2. operating according to universal principles of bioethics (Universal Declaration on Bioethics and Human Rights of UNESCO, 19 October 2005; The Charter of Fundamental rights of the EU, 2000; Helsinki Declaration of June 1964; Directive 95/46/EC; Regulation (EU) 2016/679);
3. Observance of requirements of national laws of each participant.

eTryOn will pay particular attention to issues that concern to biometric user data. More specifically, the users of our platform can generate their personal avatar in WP1 offering physical interactions with selected garments (WP2) in virtual or mixed environments (WP6, WP7). The 3D body scans can potentially allow or confirm the identification of a natural person, as they keep body measurements as 3D model, and skin color as texture. Consequently, our consortium will comply with the laws of the country where the data will be collected. Therefore, eTryOn's Ethics Board will be responsible for investigating the obligations and requirements relating to the biometrics ethics at various levels such as: i) capturing, ii) storage, iii) processing, iv) security, v) access, vi) privacy, vii) management, and viii) user's right to forget. In this direction, the protection of personal biometric data will be ensured through procedures and appropriate technologies, like the use of HTTPS protocol for the encryption of all internet transactions and appropriate European and Internet security standards from ISO, ITU, W3C, IETF and ETSI. To assure the participant's privacy, all data will be anonymized, encrypted and stored on a server to which only the relevant staff have access. More specifically the server onto which the data

[31] This would be the case when data subjects face an automatic refusal or their online credit application or e-recruiting practices without any human intervention (Recital 71 GDPR).

will be stored will have server-side encryption. That means that the server's administration personnel will be able to generate public keys for specific personnel who will have access to the data but will not be able to access the data themselves (since the private keys required for this access will be generated on the machine of the person with access to the data). This means that only the required personnel will have access to the data and even in the unlikely case of a possible data leak or server hack the data stolen will be fully encrypted and thus fully non-accessible.

### 5.3.5 Data access principles

#### Data access within institutions

The project requires the thorough validation of techniques that include the processing, storage and transfer of personal data, as described in WP1-WP8. Access to the data will be available entirely from within the participating consortium partner facilities, and in addition, only by personnel employed by those institutions. Regarding data access required for evaluation, local ethical committees will be asked for permission, taking into account the latest European guidelines. Individual institutions will therefore be required to seek appropriate approval from their national ethical organizations, but the protocol for the data access will be established centrally within the project and approved by the Project Management Board (PMB) and the Ethics Board (EB) comprising of legal and ethical experts as well as fashion industry professionals (e.g. designers, retailers), permission from which will also be required prior to the commencement of any data access.

#### Data access by other staff

Access to non-anonymized data by individuals who hold neither substantive nor honorary contracts with their institutions will not be permitted. Data available to such personnel will have originated in third-party research data- collection projects with specific ethical sanction for research use when rendered unidentifiable, and will explicitly have been consented for this usage via processes established in those projects. Key to meeting the requirements formalized in the legislations identified above is the need for significant effort into Privacy Enhancing Technologies (PETs). Several consortium members already share considerable experience of these issues from previous relevant projects, and no significant issues regarding the processes of anonymization and pseudonymization within eTryOn are foreseen. Specific protocols and evaluations will be put in place to ensure robustness, and it will be the responsibility of WP8 to provide appropriate protocols.

### 5.3.6 Data transfer principles

#### Communications between consortium members (data transfer)

Data transfer between consortium members is a requirement of several tasks within the project's technical and validation activities and, as indicated above, all such data will be rendered unidentifiable at the institution where it is acquired, and be fully consented for use. Thus, transfers between consortium members will involve only unidentifiable data, and industry-standard encryption technologies will be used within such communication systems. The eTryOn project developed advanced techniques for both centralized and federated security, ensuring system access and operation only by authorized personnel; these measures will be carried forward to eTryOn.

### 5.3.7 Provision for post-project data handling

As indicated above, within the eTryOn project, for privacy and security, no identifiable personal data will be shared outside the institutional teams of the individuals. Any such external data transfers will occur under strict security regimes, only after the data has first been rendered unidentifiable, and then only with informed consent. However, the project

is constructing communications systems that may remain viable for post-project use, so the non-identification, encryption and security systems employed will be appropriately robust so as to require no modification for any such subsequent extended usage; the overriding design stipulation is that of non- identifiable information transmission. Any such post-project usage will require further ethical sanction, in accordance with the nature of the exploitation and perpetuation mechanisms eventually envisaged.

### 5.3.8 Implementation directions in eTryOn to ensure privacy and ethical issues

Finding a balance between innovation and data protection without running the risks of over-reaction is a challenging task. Following the suggestions of (ENISA, 2015[32]), eTryOn will follow the concept of privacy and data protection by design, as a mechanism to address the privacy risks from the very beginning of the processing and apply the necessary privacy preserving solutions in the different stages of the big data value chain. Table 5.c resents an overview of the proposed designed strategies.

**Table 5.c: Privacy by design strategies**

| Strategy | Description |
|---|---|
| Minimize | The amount of personal data should be restricted to the minimal amount possible (data minimization). |
| Hide | Personal data and their interrelations should be hidden from plain view |
| Separate | Personal data should be processed in a distributed fashion, in separate compartments whenever possible |
| Aggregate | Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful |
| Inform | Data subjects should be adequately informed whenever processed (transparency) |
| Control | Data subjects should be provided agency over the processing of their personal data. |
| Enforce | A privacy policy compatible with legal requirements should be in place and should be enforced. |
| Demonstrate | Data controllers must be able to demonstrate compliance with privacy policy into force and any applicable legal requirements. |

eTryOn will implement a coherent approach to data privacy protection, taking into account the complete lifecycle of the data and its analysis envisioned in the project and best practices in the domain. Table 5.d provides an overview of the privacy by design strategies and their possible implementation measures in each of the phases of the data value chain, as these have been suggested by (ENISA, 2015).

[32] https://www.enisa.europa.eu/news/enisa-news/enisa-in-2015-annual-report

**Table 5.d: Privacy by design strategies in the data value chain**

| Data value chain | Privacy by Design Strategy | Implementation |
|---|---|---|
| Data acquisition/ collection | Minimize | Define what data are needed before collection, select before collect (reduce data fields, define relevant controls, delete unwanted information), Privacy Impact Assessments |
| | Aggregate | Local anonymization (at source) |
| | Hide | Privacy enhancing end-user tools, e.g. anti-tracking tools, encryption tools, identity masking tools, secure file sharing, etc. |
| | Inform | Provide appropriate notice to individuals – Transparency mechanisms. |
| | Control | Appropriate mechanisms for expressing consent. Opt-out mechanisms. Mechanisms for expressing privacy preferences, sticky policies, personal data stores. |
| Data analysis & data curation | Aggregate | Anonymization techniques (k-anonymity family, differential privacy). |
| | Hide | Searchable encryption, privacy preserving computations. |
| Data storage | Hide | Encryption of data at rest. Authentication and access control mechanisms. Other measures for secure data storage. |
| | Separate | Distributed/de-centralized storage and analytics facilities |
| Data use | Aggregate | Anonymization techniques. Data quality, data provenance |
| All phases | Enforce/ Demonstrate | Automated policy definition, enforcement, accountability and compliance tools. |

# 6. Health & Safety

It is unlikely that the eTryOn applications will expose participants to physical harm, since it will rely on the use of approved commercial VR glasses for the first pilot and commercial mobile devices for the other two pilots. Physiological risks however may arise (e.g. having to do with the fact that the subject is put under cognitive load and stress during a long time, or due to the immersive VR causing nausea). As part of the research ethics adopted in the eTryOn project, participants will be made aware that they can always stop their participation (also during the study). Also, negative effects for the user, although their possibility to manifest is minimal, will be analyzed and counter measures will be devised.

# 7. Conclusion

This deliverable with title “Ethical, legal and privacy requirements and guidelines for implementation” is the second deliverable regarding Work Package 8 (“Management”). Its goal was to provide a solid presentation of the techniques and services that will be used during eTryOn in order to ensure that all ethical, legal and privacy requirements are adopted throughout both the implementation of the eTryOn technologies and the interaction with end users during the piloting phase.

Two distinct categories of users will take part in the pilots (designers and customers). For both of them a different Consent Form and Information Sheet was presented. A full version of the forms will be submitted at a later stage of the project, including more details and expanding on the information currently provided.

The various data types, which will be used during the pilots, was also presented. The consortium guarantees that all personal data collected during the project will be kept secure and unreachable by unauthorized persons. The data will be handled with appropriate confidentiality and technical security, as required by law in the individual countries and EU laws and recommendations, mainly the GDPR.

The main objective of this deliverable was to give a clear and in-depth presentation on the ways that eTryOn will use in order to comply with the various principles regarding data protection. On top of that, a brief description of data protection directives and opinions at European and National level (such as General Data Protection Regulation, Directive 95/46/EC) was given. Finally, it was stated that there is not any indicator that eTryOn will expose the participants in any form of physical harm during the pilot phase.

Regarding the future steps, this deliverable will be updated in **M18**, which will also include the templates of the informed consent/assent forms and information sheets that will be used for the eTryOn pilots. The informed consents will involve description on how the data subjects will be informed of the existence of the profiling mechanism of WP3, its possible consequences and how their fundamental rights will be safeguarded.

# 8. References

## Legislation

### Council of Europe

Council of Europe, Convention for the Protection of Human Rights and fundamental Freedoms, signed in Rome, 4 November 1950

Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, Strasbourg, 28 January 1981.

### European Union

Treaty establishing the European Union, *O.J.U.E.*, 26 October 2012, C326

Treaty on the Functioning of the European Union, *O.J.E.U.*, 26 October 2012, C326.

Charter of Fundamental Rights of the European Union, *O.J.E.U.*, 18 December 2000, C364/01

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] *O.J.E.U.*, L119/1

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data [1995] *O.J.E.U.*, L281/31

## Soft law

### Article 29 Working Party

Article 29 Working Party, ‘Guidelines on Consent under regulation 2016/679’ (WP259)

Article 29 Working Party, ‘Opinion 1/2010 on the concepts of controller and processor’ (WP169)

## Case law

### European Court of Human Rights

ECtHR, *Amann v. Switzerland*, n. 27798/95, ECHR 2000-II

ECtHR, Leander v. Sweden, n. 9248/81

ECtHR, *Rotaru v. Romania*, n. 28341/95, ECHR 2000-V

### Court of Justice of the European Union

CJEU, *Peter Nowak v. Data Protection Commissioner*, case C-434/16

CJEU, *Digital Rights Ireland*, joined cases C-293/12 and C-594/12.

CJEU, *Schaible*, case C-101/12

CJEU, *Sky Österreich*, case C-283/11

CJEU, *Nelson and Others*, joined case C-581/10 and C-626/10

CJEU, *Afton Chemical*, case C-343/09

CJEU, *Volker und Markus Schecke and Eifert*, joined cases C-92/09 and C-93/09

CJEU, *Österreichischer Rundfunk and Others*, case C-465/00, C-138/01 and C-139/01

## Legal literature

De Waele H, 'Implications of Replacing the Data Protection Directive with a Regulation - a Legal Perspective' (2016) 12 Privacy & Data Protection 3

European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights' <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 14 March 2018

Kokott J and Sobotta C, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222

Purtova N, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law'

Tikkinen-Piri C, Rohunen A and Markkula J, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies' [2017] Computer Law & Security Review <http://linkinghub.elsevier.com/retrieve/pii/S0267364917301966> accessed 10 July 2017

Ustaran E, European Data Protection Law and Practice (IAPP 2018)

Varotto S and Colin J, 'The European General Data Protection Regulation and Its Potential Impact on Businesses: Some Critical Notes on the Strengthened Regime of Accountability and the New Sanctions' (2015) 20 Communication Law 78

## Other

Laurel, Brenda & Snyder, Carolyn & Quesenbery, Whitney & Wilson, Chauncey & Molich, Rolf. (2001). Ethics in HCI. 10.1145/634067.634197