COVER PAGE

Project acronym:	**DESIRE**
Project full title:	Designing the Irresistible Circular Society
Call identifier:	HORIZON-MISS-2021-NEB-01
Type of action:	CSA
Start date:	01.10.2022
End date:	30.09.2024
Grant Agreement no:	101079912

DATA MANAGEMENT PLAN - DELIVERABLE 1.2

WP1 - Task 1.1	Project management & coordination
Due date:	M6
Submission date:	31.03.20223
Dissemination level	PU
Deliverable Type	DMP
Authors:	Aase Højlund Nielsen (BXH)
Reviewers:	Alessandro Deserti (POLIMI), Martin Brynskov (DTU), Hans Jørgen Andersen (AAU)
Version:	1.0
Status:	Final

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

VERSION HISTORY

No.	Date	Description	Author/reviewers
0.1	19.03.2023	Final draft shared for review	Aase Højlund Nielsen (BXH)
0.2	27.03.2023	Feedback and comments received	Martin Brynskov (DTU), Hans Jørgen Andersen (AAU), Alessandro Deserti (POLIMI)
0.3	29.03.2023	Feedback and comments incorporated and shared with reviewers	Aase Højlund Nielsen (BXH)
1.0	31.03.2023	Final version submitted	Aase Højlund Nielsen (BXH)

ABBREVIATIONS

CESSDA	Consortium of European Social Science Data Archives
DLH	Digital Learning Hub
RRI	Responsible research and innovation
SSH	Social Sciences and Humanities
WP	Work package

Table of contents

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

LIST OF FIGURES

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

1. Introduction

This report contains the Data Management Plan (Deliverable 1.2) for DESIRE - Designing the Irresistible Circular Society. DESIRE is a Coordination and Support Action project which contributes to the objectives of Horizon Europe, more specifically to the Mission of “Climate-Neutral and Smart Cities”, and to a lesser extent the Missions of A Climate Resilient Europe and Caring for Soil is Caring for Life. The project will test principles and tools that point towards a new direction for how we build, re-build, renovate and live in cities in Europe, referring to the New European Bauhaus values of inclusion, sustainability and aesthetics and its ambition of connecting the European Green Deal to our living spaces and experiences. The project involves local transformation activities at eight different territorial sites in Europe, of which three are located in Denmark. The eight sites form eight lighthouse demonstrators where principles and tools that build on a clear bottom-up approach with co-creation and design methodologies within a learning and assessment framework that will create learning and insights to be extended to other sites and places for testing and further development after the initial 2 years.The DESIRE Digital Learning Hub frames the collected data, outputs and learnings in an open and shareable manner.

1.1 Presentation of the DMP and what it contains

As a Coordination and Support Action project, DESIRE does not produce data for the specific aim of research, but data created in DESIRE may be used in research, both within the project period and beyond, although, it is not expected that the amount of reusable datasets created in DESIRE will be significant. This Data Management Plan (DMP - D1.2) outlines the management of the created data - the organisation, storage, preservation, quality assurance and rules and procedures for sharing. The DMP also defines how the data will be made accessible and ready for interoperability and re-use based on the FAIR principles.

The DMP will function as *a living document* and be updated regularly if creation of new data sets or changes in the organisation, storage and access to the data occurs.

This first version of the DMP has been developed with input from key partners in the DESIRE consortium.

1.2 The structure of the document

The DMP follows closely the template provided by the European Commission, and answers all relevant questions within this.

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement N° 101079912.

2. Data Summary

2.1 Re-use of existing data

Re-use of existing data, e.g. transformation plans, reports, analysis and data relating directly to the status of the 8 different territorial sites, may be considered in particular to support the need for conducting analyses of baselines.

2.2 Types and formats of data

The project will generate data of three different kinds, defined with specific reference to the framework set by the New European Bauhaus: 'Materials' represent the aesthetic parts of DESIRE, 'Typologies of places and interaction' refer to inclusion, and 'Circularity and sustainability' relates to sustainability. The following presents an outline of the expected data formats and types that will be created within each overall typology:

I. Materials

- Workshop material, digital and analogue, e.g. boards, cards for reflections and notes, post-its, and their digital representation (photos of physical material)
- Artistic expressions, exhibitions - documented through photos, video and sound recordings
- Design-based and co-created tools and methods - represented through formalised and codified descriptions

II. Typologies of places and interactions

- Eight different local territorial sites with their specific characteristics. Represented through transformation plans, prototypes, mock-ups, social media interactions, living lab, etc.
- Data generated through the engagement tool ('Our Walk App') - photos, comments and interactions generated through dialogues and workshops
- Local interactions involving the ecosystems of the eight different territorial sites - notes, photos, manifestations of interactions in the sense of video recordings, etc.
- Interactions with a broader community (business, local, regional and national authorities, NGOs, etc) - expressions of interest, Memorandum of Understanding, agreement on actions

III. Circularity and sustainability

- Re-use of material - documents and photos describing and listing re-use of material
- Behavioural change, change of mindset - interviews, surveys, written statements or photos of actions and decisions representing a change in behaviour
- CO_2 reduction - estimates of CO_2 reduction options, analyses of CO_2 emissions

2.3 The purpose of data generation and the relation to the objectives of the project

The data generation serves three main purposes:

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

a) Present learnings and assessment of the application of principles and tools applied in the context of the project and the project objectives
b) Supporting the double loop learning framework where the development of the project specific approach form a key element of the overall learning objective of the project
c) Analysing transformation activities at each of the 8 territorial sites to assess local impact

2.4 The expected size of the data

As the data sets created during the project differ in type, format and extent it will not be possible to state what the expected size will be. However, as main parts of the data are expected to consist of digitised text and images (photos, plans, etc) no specific requirements regarding storage are expected.

2.5 The origin/provenance of the data

The provenance of the main part of the data, both generated and re-used, will relate to the geographical location of the eight territorial sites: Kalundborg city, Herlev Asphalt Factory, Gadehavegaard (Høje-Taastrup), Ziepju Street (Riga), BTC City Center (Ljubljana), MIND (Milan), Cascina Falchera (Turin) and Wildemannbuurt (Amsterdam). It will refer to the location, the date and time, and the beneficiaries/external stakeholders involved in the creation of the data.

The provenance or origin created as part of activities surrounding what will be going on at the 8 territorial sites will refer to the specific WP, task, date/time and beneficiary producing the data.

2.6 Data utility

Data utility is expected to concern, among others, city planners, decision makers at city level, and researchers within social science and humanities, especially within domains of strategic urban development and citizens participatory processes.

3. FAIR data

DESIRE will ensure that the generated research data is findable, accessible, interoperable and reusable (FAIR), complying with the EU Guidelines on FAIR Data Management[1].

[1] Guidelines on FAIR Data Management in Horizon 2020, version 3.0, 26 July 2016, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf (Accessed March 13th, 2023)

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

3.1. Making data findable, including provisions for metadata

3.1.1 Persistent identifier

Persistent identifiers will be considered for data sets that during the collection are considered important for future research and utility. The responsibility of this lies with the researchers involved in the project, primarily researchers directly involved in activities relating to transformation and demonstration (WP3) and learning and assessment (WP4).
Submission to a public repository will provide the persistent identifier to the data where it is considered relevant. See section 3.2.1 for more information of choice of repository.

3.1.2 Metadata and standards

Metadata standards are not available for the disciplines or research domains encompassing the DESIRE project. This has been documented through a search at FAIRsharing. Therefore, a manually defined set of metadata has been created, distinguishing between administrative, descriptive and structural metadata[2]:

- *Structural metadata*: the internal structure of the data and data on how the data was created (e.g. categories, sample unit, collection method)
- *Descriptive metadata*: data that allow other people to identify the data (e.g. the title, author, abstract, persistent identifier,...)
- *Administrative metadata*: data about the project relevant for managing the data (e.g. project period, funder, collaborator, …)

Templates containing metadata will be applied and adjusted according to the different types of data set - see annex 1 for an example.

In addition to this, tables with descriptive metadata, e.g. version history, search keywords, and abstract, and structural metadata, e.g. date and time(stamps), method of collection, categories of data, will be applied. See fig.1 for an example of descriptive and administrative metadata.

[2] D.B. Deutz, M.C.H. Buss, J. S. Hansen, K. K. Hansen, K.G. Kjelmann, A.V. Larsen, E. Vlachos, K.F. Holmstrand (2020). How to FAIR: a Danish website to guide researchers on making research data more FAIR **https://doi.org/10.5281/zenodo.3712065** - https://howtofair.dk [accessed February 14th, 2023]

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

Project acronym:	DESIRE
Project full title:	Designing the Irresistible Circular Society
Call identifier:	HORIZON-MISS-2021-NEB-01
Type of action:	CSA
Start date:	01.10.2022
End date:	30.09.2024
Grant Agreement no:	101079912

[NAME OF DELIVERABLE] - DELIVERABLE x.x

WP x - Task x.x	[name of WP]
Due date:	[insert date + month number, e.g. M6]
Submission date:	[date]
Dissemination level	PU
Deliverable Type	Report
Authors:	[names of authors + organisation abbreviation, e.g. Aase Højlund Nielsen (BXH)]
Reviewers:	[name of reviewers and role in DESIRE, e.g. xx (WP4-leader), xx (expert organisation)]
Version:	[number, e.g. 1.2]
Status:	[status during the process, e.g. draft, final]

Fig. 1. Example of table containing administrative and descriptive metadata

3.1.3 Search keywords

A list of search keywords is offered as part of the descriptive metadata. The list is based on the keywords that were chosen as part of the development of the proposal and as such, it is aligned with the vocabulary used with reference to Horizon Europe and New European Bauhaus.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

3.1.4 Harvesting and indexing of metadata

Using rich descriptive metadata (e.g. search keywords, title, authors) will make the metadata accessible. Harvesting and indexing will be possible for those data being stored publicly, either through the project website or through repositories ensuring access and preservation.

3.2 Accessibility

3.2.1 Repository

3.2.1.1 Trusted repository

The repositories used by the universities involved in this project (Politecnico di Milano, Aalborg University, Denmark's Technical University, Royal Danish Academy) are bound in contracts and policies that makes it difficult for external users to access them for data created in DESIRE. Therefore, alternative trusted repository spaces compliant with the EU policies will be identified and taken into use, where needed.

The majority of data created within DESIRE will be created during activities taking place at the 8 local sites. Each beneficiary involved with these sites and responsible for the activities will be responsible for depositing the data at a trusted repository where the data will be accessible, also beyond the project period. As not all of these beneficiaries will have immediate access to a trusted repository, alternative solutions for storing data in a trusted repository will be investigated by the Coordinator in close collaboration with primarily WP3 and WP4 leads (AAU and POLIMI), involved directly in site related activities.

3.2.1.2 Exploration of appropriate arrangements with the identified repository

The possibility of offering the trusted repository of AAU (WP3 lead, coordinating activities at the different sites) as a trusted repository for those beneficiaries with no immediate access to a trusted repository has been explored at a preliminary level. Further clarification will be performed to settle appropriate arrangements, if needed (see also section 6.1).

3.2.1.3 Assignment of identifiers

Assignments of identifiers depend on i) an individual assessment of the dataset in question and ii) opportunities for assigning identifiers within the chosen trusted repositories. DESIRE datasets may be assigned e.g. a DOI if considered appropriate in relation to the value and importance of the dataset.

3.2.2 Data

3.2.2.1 Open access to data

It is not anticipated that data generated as part of the project will be restricted for access.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

DESIRE rests on an open-project approach that emphasises openness and transparency in all its interactions and processes. This aligns with the fundamental methodological design approach, the general ambition of learning through sharing, and the adoption of co-creation as a framework to operationalize RRI. The Digital Learning Hub that DESIRE will develop forms the gateway to all parts of the project and gives free access for all to interactions, co-created tools and principles and the aggregated learnings and
evaluation outcomes and exploitation and scaling activities.

3.2.2.2 Embargo to give time to publish or seek protection of the intellectual property

N/A

3.2.2.3 Accessibility through free and standardized access protocol

Access to the data through a free and standardized access protocol will be discussed as part of the data management activities, and decisions will be made with reference to the relevance of the data and how it will be stored.

3.2.2.4 Restriction on use

No restriction on use is expected, neither during the project or beyond.

3.2.2.5 Ascertain of the identity of the person accessing the data

As DESIRE claims to provide open access to all data generated in the project, it will not be needed to ascertain the identity of persons accessing the data.

3.2.2.6 Data access committee

As DESIRE is not expected to produce any sensitive data, a need for a data access committee is not anticipated. However, if this situation changes, the Coordinator in collaboration with the members of the Executive Board will present appropriate means to take action.

3.2.3 Metadata

3.2.3.1 Availability of metadata

Metadata will be made openly available, licensed under the latest available version of the Creative Commons Attribution International Public Licence (CC BY) as stipulated in the Grant Agreement, Article 17. The metadata has been further described in section 3.1.2 - this information is considered sufficient to enable users accessing the data.

3.2.3.2 Duration of the availability of the data and metadata

Data and metadata linked with datasets that will be deposited in the chosen repository (see section 3.2.1.1) will remain available and findable also beyond the project period. The

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

availability of the metadata also beyond the availability of the data depends on the policies of the used repositories.

3.2.3.3 Need for documentation or reference about software to access or read the data

Only data deriving from the engagement tool ('Our Walk App') may require specific documentation or reference to be used as part of a site's activities, but it can be accessed, also interactively, like all other data is expected to be, through open web and file formats like pdf, ppt, txt, jpg which are generally accessible license-free.

If other data is created that requires specific software for access or reading, documentation and reference to specific software will be defined.

3.3 Interoperability

3.3.1 Data and metadata vocabularies, standards, formats and methodologies

DESIRE does not anticipate a need for developing data models or specific metadata vocabularies or standards. The interoperability will be ensured by using existing formats like those defined in section 3.2.3.3 and by giving access through pre-defined and searchable keywords. Further, if data created during the project uses non-standard data format, a reference to the software that can be run to transform it into a community-endorsed data standard will be provided.

It might be considered to use standards set by for instance CESSDA, a European Research Infrastructure Consortium providing services to researchers within SSH. The decision will be made depending on the type of collected data.

3.3.2 Uncommon or project specific generates ontologies or vocabularies

N/A

3.3.3 Inclusion of qualified references[3] to other data

N/A

3.4 Re-use of data

3.4.1 Documentation needed to validate data analysis and facilitate data re-use

Documentation will be provided to ensure accuracy in data validation, e.g. through metadata descriptions. Readme files might be provided on datasets of e.g. photos, plans or for

[3] *A qualified reference is a cross-reference that explains its intent. For example, X is regulator of Y is a much more qualified reference than X is associated with Y, or X see also Y. The goal therefore is to create as many meaningful links as possible between (meta)data resources to enrich the contextual knowledge about the data. (Source: https://www.go-fair.org/fair-principles/i3-metadata-include-qualified-references-metadata/)*

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

instance data created through the 'Our Walk App'. The readme files will contain information relating to metadata and on the methodology behind the collection and analysis of data.

3.4.2 Free availability of data in the public domain to permit the widest re-use possible

Data that is non-sensitive and generated through the project will be made freely available through the Digital Learning Hub which is created as part of the project. The licensing of the data will follow the Creative Commons license as defined in section 3.2.3.1 and be in line with the obligations in the Grant Agreement. Data may also be available through the depository chosen as a trusted repository of the data (see section 3.2.1.1) Decisions on where the data will be accessible will depend on the type of data, the data quality and the relevance of the storage options.

3.4.3 Data accessed and used by third parties

Data that can be accessed through the Digital Learning Hub will be usable by third parties, both during the project and after, depending on how and for how long the DLH will be sustained and maintained. Decisions on sustain and maintenance of the hub will be an integral part of the revisions of the Exploitation Strategy (D6.1) and partly also the Financial Plan (D6.2) which will support the extension and scaling of the project.

Data or dataset considered of relevance for third parties may also be deposited at the chosen trusted repository (see sections 3.2.1.1 and 3.4.2).

3.4.4 Documentation of the provenance of the data

The provenance of most of the data created in DESIRE will be documented through the applied metadata. Regarding the data created through 'Our Walk App' and the datascapes displaying learnings based on the data, the documentation of the provenance will be an integrated part of the app ensuring track of the data from when it is created and through different applications embedded in the application.

4. Other research outputs

DESIRE plans different outputs which will be research based and building on data created throughout the project. It concerns e.g. Innovation Biographies (a case study presenting successful practices - D4.3) and Narratives of irresistible circular futures (white paper based on aggregation of learnings from the demonstrations at the different sites - D3.3). The management of these research outputs will be done in line with the overall research management plans in place at the different involved institutions and following the FAIR principles. Detailed plans for managing and sharing will be provided, if needed, in collaboration with the involved institutions. These plans will be considered along the process of preparing the specific research outputs.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

In addition to this, all research outputs will be stored at the Digital Learning Hub and at the trusted repository (see section 3.2.1.1).

5. Allocation of resources

5.1. Costs for making data or other research outputs FAIR

The costs for making the data FAIR is an integral part of the activities leading up to the establishment of a Digital Learning Hub which is one of the main outputs of the project. Decisions on how to maintain and sustain the Digital Learning Hub will be integrated in the process of implementing and adapting the Exploitation Strategy and Plan, including developing a financial plan to support the extension and scaling of the DESIRE initiative.

Eventual costs that go beyond the Digital Learning Hub, e.g. costs for assignment of pertinent identifiers, data validation and transaction using blockchain technology (e.g. bloxberg), will be analysed if the created datasets or research outputs make it relevant to consider. These analyses will form part of considerations that concern scaling of the DESIRE activities and outputs.

5.2 Cover of costs

The costs for the Digital Learning Hub will be covered through the DESIRE project grant. Costs that go beyond the Digital Learning Hub will be addressed by the consortium, and primarily the involved research partners, if and when it is considered relevant and necessary. Decisions will be based on considerations regarding relevance, added value and available sources.

5.3 Responsibility for data management

The responsibility for data management lies with the Project Coordinator (BLOXHUB), also responsible for adjusting and further developing the Data Management Plan. The responsibility will be conducted in close collaboration with the involved research institutions (primarily POLIMI, AAU and DTU, all involved in activities relating to data creation and data application for research purposes).

5.4 Long term preservation

A long term preservation of the created data is considered possible according to following key parameters:

- I: A scaling framework is one of three objectives of DESIRE. In addition to this, a financial plan supporting the scaling of the DESIRE results and learnings forms an important milestone and deliverable, preparing the ground for long term relevance and preservation of the data created in DESIRE
- II: The consortium behind DESIRE comprises strong research institutions like POLIMI, AAU, DTU and the Royal Danish Academy. The departments involved in DESIRE are all dedicated to research in design, architecture, creativity and urban transformation - this sets a basic foundation for a long term interest in the data

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

created and therefore an interest in identifying solutions for finding the necessary resources

- III: DESIRE is just one of several European initiatives and projects supporting the New European Bauhaus initiative. Considering the strength that this initiative has achieved during a relatively short period of time (launched in September 2020) and the ambitions it builds on, the request and need for data created through the DESIRE experimentation is expected to be of long term importance, which supports the ambition of finding long term preservation solutions.

Decisions on responsibility, which dataset should be kept and the actual management role must await the experimentation of activities and the actual creation of data. This means that considerations about long term preservation will be initiated at a later stage of the project.

6. Data security

6.1 Provisions in place for data security

Data will be checked for compliance with GDPR before being deposited. The responsibility for compliance with GDPR lies with the individual organisation depositing data in the DESIRE repository.

Instructions on how to ensure compliance with GDPR will be prepared and shared with all territorial sites when the demonstration phase gets started (from M7 - April 2023). AAU (WP3 lead) will bear the main responsibility for this action, supported by the Coordinator.

All organisations responsible for activities at the different territorial sites will act as ‘data controllers’, meaning that they will be responsible for storing data created during these activities in alignment with national and European legislation on personal data. A guideline on how to ensure a sufficient level of data security will be prepared prior to the activities. Main responsibility for preparing the guidelines lie with AAU (WP3 lead), in close collaboration with the coordinator.

As data security also concerns storage of data in compliance with EU regulations, a process will be initiated to ensure that all sites are aware of their data responsibility:

1) Identification of repositories in use at the different sites organisations
2) In cases where the existing repository doesn’t comply with the data security requirements, access to a trusted repository, e.g. at AAU, will be offered based on a signed agreement
3) A data processing agreement concludes the arrangement between the owner of a trusted repository and the concerned site organisation (see annex 3 for an example, using AAU as trusted repository) in cases where the site organisation accepts the provided

6.2 Storage of data in trusted repositories for long term preservation and curation

See 3.2.1, 5.4 and 6.1.

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement N° 101079912.

In relation to the user engagement tool ('Our Walk App') that will be applied to collect data from external sources (citizens, stakeholders, local authorities, etc) and used for dialogues and participatory activities, a privacy policy has been developed to ensure compliance with the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR). The privacy policy states the use of the data collected and each participant's access to own data, also to withdrawal of their personal data.

Data collected through the 'Our Walk App' will comply with the overall ethical conditions underlying the creation, storage and use of data in DESIRE. This means that data will be anonymised to be sharable with third users. Decisions on long term preservation and curation of this data, including depositing, will be defined as part of the overall decision making on accessibility and preservation of data (see chapter 5).

7. Ethics

Procedures on how to manage consensus on the use of data will be established along with templates to ensure 'informed consent'. The Coordinator in close collaboration with the involved research institution will be responsible for creating awareness among the involved parties for the importance of managing consensus on the use of data and for obtaining consent from external participants for storing and using data created through activities.

Any activity that involves human participants, e.g. workshops, interviews, questionnaires, will be conducted on the basis of 'informed consent'. This includes that any participation will be voluntary and free from coercion; that participants will contribute under the conditions of non-attributable information to guarantee the anonymity of the participants; that participants will not contribute without their knowledge and consent; and that participants will have the right to withdraw at any time. These principles will be included in the information sheet enclosed with the consent form (see annex 2 for an example of an 'informed consent form'). Furthermore, participants will be made aware of the overall nature of the project, and the conventions and rules that govern design-enabled innovation design methods and social science research, when relevant.

Activities that involve interviews and workshops will be governed by the academic conventions governing these methodologies, including information about the conditions under which the participants are being asked to provide information, and the ways in which the findings will be stored, processed and presented, according to the latest version of the DMP. Moreover, data will be anonymised where appropriate.

Guidelines that support the beneficiaries in their compliance with these ethical standards will be provided and shared as from M7, when the demonstration activities initiate. The 'informed consent form' will be adapted into the different national contexts and languages. An initial version in English is ready at the DESIRE drive, and versions in local languages will be made available online, accessible to the beneficiaries when needed. The Coordinator is

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

responsible for providing an 'informed consent form' and guidelines will be developed as a co-created activity involving primarily WP3 and WP4 leads (AAU and POLIMI).

8. Other issues

N/A

ANNEX

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

ANNEX 1 - Example of metadata template

METADATA TEMPLATE (example)

Administrative metadata

Project acronym:	**DESIRE**
Project full title:	Designing the Irresistible Circular Society
Call identifier:	HORIZON-MISS-2021-NEB-01
Type of action:	CSA
Start date:	01.10.2022
End date:	30.09.2024
Grant Agreement no:	101079912

Structural metadata

Category(ies) of data	*e.g. Photos*
Data formats	*e.g. jpg*
Data structure	*e.g. structured according to themes*
Collection method	*e.g. Produced as part of co-creation sessions*

Descriptive metadata

Title of the data	*e.g. Co-creation activities at XX*
Author/creator of the data	*[name]*
Date/time of the creation of data	*[time, date, year when the photos were taken]*
Abstract	*[short text describing the data]*
Keywords	*[searchable keywords]*

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

ANNEX 2 - Example of informed consent form

INFORMED CONSENT FORM - example

Information sheet and consent form to take part in a workshop in [country]

Title of the project: DESIRE - Designing the irresistible circular society
Funding: European Union's Horizon Europe (HORIZON-MISS-2021-NEB-01)

Name and contact details of the partner involved in DESIRE
[name, title]
[organisation]
[e-mail address]

Name of principal investigator (PI)
[name]
Aalborg University or Politecnico di Milano
[e-mail address]
[phone number - can be left out]

Invitation
We would like to invite you to take part in our project. I will go through this information sheet with you, to help you decide whether or not you would like to take part and answer any questions you may have. I would suggest this should take about 10 minutes. Do ask if anything is unclear. Please feel free to talk to others about the project if you wish.
I am [name of person requesting consent] and I work at [name of organisation] taking part in DESIRE - Designing the irresistible circular society, a project funded through the European Union's Horizon Europe programme.

Purpose of the project
DESIRE - Designing the Irresistible Circular Society contributes to the objectives of Horizon Europe, more specifically to the EU mission of delivering 100 climate-neutral and smart cities within 2030. The project will test principles and tools that point towards a new direction for how we build, re-build, renovate and live in cities in Europe, referring to the New European Bauhaus values of inclusion, sustainability and aesthetics and its ambition of connecting the European Green Deal to our living spaces and experiences. The partners will share the experience gained from DESIRE via an electronic learning platform so that others can draw inspiration from it.

Your participation
Thanks in advance for being available for taking part in [the workshop/interview/activity]. If you agree to take part, we will ask you to sign the participant consent form. As a volunteer you can stop your participation at any time, without giving a reason if you do not wish to.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

Collected data
During [the workshop/interview/activity] you will be invited to express your experiences, opinions and ideas on the applied principles and tools we are testing, and how to transform this site according to the principles of New European Bauhaus (inclusion, aesthetics and sustainability). The [workshop/interview/activity] will be in [language], it will be video / audio recorded and transcribed, (and pictures and posters will be produced). During the [activity] you can request to stop the recording at any point. Verbatim comments extracted from the transcript can be used only within the scope of the project. The data will be collected, stored and processes in compliance with the European Union Regulation (GDPR - 2016/679), and with the [country] legislation (*ref. to relevant legislation*).

Confidentiality
Data from the activity (photos, videos, documents drawn up during the meeting, transcription of verbal interactions) will be used for dissemination and communication on project websites and social media channels (e.g. Facebook, Twitter, Instagram, and others). Data may also be used in other dissemination activities, such as dissemination workshops, conference papers, and in both magazine and academic journals. Transcription of verbal interactions and documents drawn up during the meeting will be used in an anonymized form. We may disclose your role within the organisation of which you are member. The anonymity of the organisation will be guaranteed in case you ask for that.

Data storage and protection
The research data and signed consent forms will be retained in the following formats: either paper copies or electronic. The papers will be kept in a locked filing cabinet at [name of DESIRE beneficiary]. The video/audio-recorded files will be stored in a password protected storage driver which will be kept in a locked filing cabinet at [name of DESIRE beneficiary]. Data may be presented to others at conferences, or published as a project report or in academic journals, books and magazine. They could also be made available to the funder of the research.

What if there is a problem?
If you have a query, concern or complaint about any aspect of this project, please contact the Principal Investigator and the DESIRE partner you have been in contact with. The contact details for both the DESIRE partner and the PI are detailed on page 1.

Funding
This project is being funded by the European Union's Horizon Europe programme (HORIZON-MISS-2021-NEB-01, Grant No. 101079912). None of the researchers or project staff will receive any financial reward by conducting this [activity/workshop], other than their normal salary.

Thank you
Thank you for taking time to read this information sheet and for considering volunteering for this research. If you do agree to participate your consent will be sought; please see the accompanying consent form. You will then be given a copy of this information sheet and

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

your signed consent form.

Date,

Informed consent form to take part in an interview

	Add your initials next to the statement
I confirm that I have read and understand the information sheet dated [*insert date*] explaining the above project and I have had the opportunity to ask questions about the project.	
I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason and without there being any negative consequences. To do so, please contact the Principal Investigator via email or telephone at the contact details provided. In addition, should I not wish to answer any particular question or questions, I am free to decline. If I do withdraw from the project after some data have been collected, I will be asked if I am content for the data collected thus far to be retained and included in the project. Once the project has been completed, and the data analysed, it will not be possible to withdraw my data from the project.	
I give permission for members of the project team to have access to my responses. I have the right to be anonymous. I understand that my role within the organisation of which I'm member could be disclosed. I understand that I can require to preserve the anonymity of the organization of which I'm member.	
I agree for the data collected from me to be stored and used in relevant future research in an anonymized form.	
I understand that other genuine researchers will have access to this data onlyif they agree to preserve the confidentiality of the information as requested inthis form.	
I understand that other researchers may use my words in publications, reports, web pages, and other project outputs, only	

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

if they agree to preserve the confidentiality of the information as requested in this form.	
I understand that relevant sections of the data collected during the project maybe looked at by auditors from University College London where it is relevant for the audit. I give permission for these individuals to have access to my records.	

Name of participant	
Participant's signature	
Date	
Name of interviewer	
Signature	

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

ANNEX 3 - Example of data processing agreement

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101079912.

[DESIRE – D1.2 ANNEX 3 - EXAMPLE]

DATA PROCESSING AGREEMENT

between
Aalborg University
CVR number 29102384
Insert the name of the institution or administrative entity;
Fredrik Bajers Vej 7k
9220 Aalborg
Denmark
(hereinafter “the controller”)

and

Company/institution’s name and possibly corporate form (A/S, ApS, etc.)
CVR number XXXXXXXX
Address
Postcode location
hereinafter referred to as the “processor”)

each of them is a “party” and together make up the “Parties”.

Has STATED the following standard contractual clauses (the Clauses) in order to comply with the General Data Protection Regulation and to ensure the protection of privacy and fundamental rights and freedoms of natural persons.

1. TABLE OF CONTENTS

THE PREAMBLE

1. These provisions lay down the rights and obligations of the processor when carrying out the processing of personal data on behalf of the controller.

2. These provisions are designed to comply with Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Privacy Regulation).

3. In the context of [Describe Processing Activity], the Processor processes personal data on behalf of the Data Controller in accordance with these Provisions.

4. The provisions shall prevail over any equivalent provisions of other agreements between the parties.

5. There are four annexes to these provisions and the Annexes form an integral part of the provisions.

6. Annex A provides details on the processing of personal data, including on the purpose and nature of the processing, the type of personal data, the categories of data subjects and the duration of the processing.

7. Annex B sets out the controller's conditions for the processor's use of sub-processors and a list of sub-processors for which the controller has authorised the use.

8. Annex C sets out the instructions of the controller with regard to the processing of personal data by the processor, a description of the minimum security measures to be implemented by the processor and the supervision of the processor and any sub-processors.

9. The provisions and related annexes shall be kept in writing, including electronically, by both Parties.

10. These provisions do not release the Data Processor from obligations imposed on the Data Processor under the General Data Protection Regulation or any other legislation.

2. RIGHTS AND OBLIGATIONS OF THE CONTROLLER

1. The controller is responsible for ensuring that the processing of personal data is carried out in accordance with the General Data Protection Regulation (see Article 24 of the GDPR), data protection provisions of other Union or Member State[1] law and these provisions.

2. The controller has the right and the obligation to make decisions about the purposes and means of the processing of personal data.

1 References to "Member State" in these provisions shall be understood as referring to "EEA Member States".

3. The controller is responsible for ensuring, among other things, that there is a basis for the processing of personal data that the processor is instructed to carry out.

3. THE DATA PROCESSOR ACTS ON INSTRUCTIONS

1. The processor may only process personal data on documented instructions from the controller, unless required by Union or Member State law to which the processor is subject. This instruction shall be specified in Annexes A and C. Subsequent instructions may also be given by the controller while processing personal data, but the instruction must always be documented and kept in writing, including by electronic means, together with these provisions.

2. The processor shall immediately inform the controller if, in its opinion, an instruction is contrary to this Regulation or to data protection provisions of other Union or Member State law.

4. CONFIDENTIALITY

1. The processor may only grant access to personal data processed on behalf of the controller to persons who are subject to the processor's instructional powers, who have committed to confidentiality or are subject to an appropriate legal obligation of confidentiality, and only to the extent necessary. The list of persons to whom access has been granted shall be reviewed on an ongoing basis. On the basis of this review, access to personal data may be closed if the access is no longer necessary and the personal data must no longer be accessible to those persons.

2. The processor shall, at the request of the controller, be able to demonstrate that the persons concerned, who are subject to the powers of instruction of the processor, are subject to the above-mentioned obligation of professional secrecy.

5. SAFETY OF TREATMENT

1. Article 32 of the GDPR states that the controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing concerned, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, shall implement appropriate technical and organisational measures to ensure a level of protection appropriate to those risks.

   The controller shall assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to address those risks. Depending on their relevance, this may include:

   a. Pseudonymisation and encryption of personal data

   b. ability to ensure the continuous confidentiality, integrity, availability and robustness of processing systems and services;

   c. ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a procedure for the regular testing, assessment and evaluation of the effectiveness of the technical and organisational measures to ensure the security of processing.

2. Article 32 of the Regulation also requires the processor to assess — independently of the controller — the risks to the rights of natural persons that the processing poses and implement measures to address those risks. For the purposes of this assessment, the controller shall make available to the processor the necessary information enabling him or her to identify and assess such risks.

3. In addition, the processor shall assist the controller in its compliance with the controller's obligation under Article 32 of the Regulation by, inter alia, providing the controller with the necessary information regarding the technical and organisational security measures already implemented by the processor pursuant to Article 32 of the Regulation and any other information necessary for the controller's compliance with its obligation under Article 32 of the Regulation.

The security of processing is described in more detail in Annex C.2, which also lists the minimum measures to be implemented by the processor. Where the controller further requires identified risks and consequences, these will also be set out in Annex C.2.

6. USE OF SUB-PROCESSORS

1. The processor must comply with the conditions referred to in Article 28(2) and (4) of the GDPR in order to make use of another processor (a sub-processor).

2. Thus, the Data Processor may not make use of a Sub-Processor for the fulfilment of these Provisions without the prior specific written consent of the Data Controller.

3. The processor may only make use of sub-processors with the prior specific written consent of the controller. The processor shall submit the request for a specific authorisation at least 4 weeks before the use of that sub-processor. The list of sub-processors already authorised by the controller is set out in Annex B.

4. Where the processor makes use of a sub-processor in carrying out specific processing activities on behalf of the controller, the processor shall, by means of a contract or other legal document under Union or Member State law, impose on the sub-processor the same data protection obligations as those set out in those provisions, providing in particular appropriate safeguards that the sub-processor will implement the technical and organisational measures in such a way that the processing complies with the requirements of these Provisions and the GDPR.

The Data Processor is therefore responsible for requiring that the Sub-Processor at least comply with the Data Processor's obligations under these Conditions and the General Data Protection Regulation.

5. The Sub-Processor Agreement(s) and any subsequent changes thereto shall be transmitted, at the request of the Data Controller, in copy to the Data Controller, who thereby has the opportunity to ensure that equivalent data protection obligations resulting from these Provisions are imposed on the Sub-Processor. Provisions on

commercial terms that do not affect the data protection content of the sub-processor agreement shall not be sent to the controller.

6. In its agreement with the sub-processor, the processor shall include the controller as a beneficiary third party in the event of the processor's bankruptcy, so that the controller can sub-processor rights and assert them against sub-processors, which, for example, enables the controller to instruct the sub-processor to erase or return the personal data.

7. If the Sub-Processor does not comply with its data protection obligations, the Data Processor remains fully accountable to the Data Controller for the fulfilment of the Sub-Processor's obligations. This does not affect the rights of data subjects arising from the GDPR, in particular Articles 79 and 82 thereof, vis-à-vis the controller and the processor, including the sub-processor.

7. TRANSFER TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

1. Any transfer of personal data to third countries or international organisations may only be carried out by the processor on the basis of documented instructions from the controller and must always be carried out in accordance with Chapter V of the GDPR.

2. Where the transfer of personal data to third countries or international organisations to which the processor has not been instructed by the controller is required by Union or Member State law to which the processor is subject, the processor shall inform the controller of that legal requirement prior to processing, unless that law prohibits such notification for reasons of important public interest.

3. Thus, without documented instructions from the controller, the processor cannot, within the scope of these provisions:

    a. transfer personal data to a controller or processor in a third country or an international organisation;
    b. entrust the processing of personal data to a sub-processor in a third country;
    c. processing the personal data in a third country;

4. The instructions of the controller concerning the transfer of personal data to a third country, including the possible basis for the transfer in Chapter V of the GDPR on which the transfer is based, shall be set out in Annex C.6.

5. These provisions are not to be confused with standard contractual clauses within the meaning of Article 46(2)(c) and (d) of the GDPR, and these provisions cannot constitute a basis for the transfer of personal data within the meaning of Chapter V of the GDPR.

8. ASSISTANCE TO THE CONTROLLER

1. The processor shall, taking into account the nature of the processing, assist the controller, as far as possible, by means of appropriate technical and organisational measures, in fulfilling the controller's obligation to respond to requests for the exercise of data subjects' rights as set out in Chapter III of the GDPR.

This implies that the processor shall, as far as possible, assist the controller in ensuring compliance with:

a. the obligation to provide information when collecting personal data from the data subject
b. the obligation to provide information if personal data have not been collected from the data subject;
c. right of access
d. right to rectification
e. the right to erasure ("right to be forgotten")
f. right to restriction of processing
g. obligation to notify in connection with rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be the subject of a decision based solely on automated processing, including profiling;

2. In addition to the Data Processor's obligation to assist the controller in accordance with Clause 6.3., the Data Processor shall further, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller with:

a. the obligation of the controller to notify the personal data breach without undue delay and, where possible, no later than 72 hours after it has become aware, to the competent supervisory authority, the Data Protection Agency, unless it is unlikely that the personal data breach entails a risk to the rights or freedoms of natural persons;

b. the obligation of the controller to inform the data subject of a personal data breach without undue delay where the breach is likely to result in a high risk to the rights and freedoms of natural persons;

c. the obligation of the controller to carry out, prior to the processing, an analysis of the consequences of the envisaged processing operations on the protection of personal data (an impact assessment);

d. the controller's obligation to consult the competent supervisory authority, the Data Protection Agency, prior to processing, if a data protection impact assessment shows that the processing would lead to a high risk in the absence of measures taken by the controller to mitigate the risk.

3. The Parties have set out in Annex C the necessary technical and organisational measures by which the processor shall assist the controller, as well as to what extent and extent. This applies to the obligations arising from Provisions 9.1. and 9.2.

9. NOTIFICATION OF PERSONAL DATA BREACHES

1. The processor shall inform the controller without undue delay after becoming aware of a personal data breach.

2. The data processor's notification to the controller shall, where possible, be made by the processor providing an initial notification as soon as possible and no later than 4 hours after it has become aware of the breach and a detailed notification as soon as possible and at the latest within 36 hours after the processor is aware of the

breach, so that the controller can comply with its obligation to notify the personal data breach to the competent supervisory authority in accordance with Article 33 of the GDPR.

3. In accordance with Clause 9.2.a, the processor shall assist the controller in reporting the breach to the competent supervisory authority. This means that the processor must assist in providing the following information, which according to Article 33(3) must be included in the controller's notification of the breach to the competent supervisory authority:

    a. the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, as well as the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed by the controller to address the personal data breach, including, where appropriate, measures to limit its possible adverse effects.

4. The Parties shall specify in Annex C the information to be provided by the processor in the context of its assistance to the controller in its obligation to notify personal data breaches to the competent supervisory authority.

10. DELETION AND RETURN OF INFORMATION

1. Upon termination of the processing of personal data by the processor, the processor shall erase all personal data which have been processed on behalf of the controller and confirm to the controller that the data have been erased / [VAC 2] return all the personal data and delete existing copies, unless Union or Member State law provides for the retention of the personal data.

2. [If RELEVANT] The following rules of Union law, Member States' national law or codes of conduct provide for the retention of personal data after termination of the services relating to the processing of personal data:

    a. [...] e.g. The Danish Code of Conduct for Research Integrity, after which data must be retained for a period of at least 5 years from the date of publication.

    b. for example, the Accounting Act, according to which information relating to a payment must be kept for 5 years from the end of the financial year to which the material relates.

The Data Processor undertakes to process the Personal Data only for the purpose(s) for the period and under the conditions laid down in these Rules.

11. AUDIT, INCLUDING INSPECTION

1. The processor shall make available to the controller all information necessary to demonstrate compliance with Article 28 of the GDPR and these Provisions and provides for and contributes to audits, including inspections carried out by the controller or another auditor authorised by the controller.

2. The procedures for the controller's audits, including inspections, with the processor and sub-processors are specified in Annexes C.7. and C.8.

3. The Data Processor is obliged to provide supervisory authorities who, under applicable law, have access to the facilities of the controller or processor, or representatives acting on behalf of the supervisory authority, access to the Data Processor's physical facilities against due identification.

12. AGREEMENT OF THE PARTIES ON OTHER MATTERS

1. The parties may agree on other provisions relating to the processing of personal data, such as liability, as long as these other provisions do not directly or indirectly conflict with the provisions or adversely affect the fundamental rights and freedoms of the data subject resulting from the General Data Protection Regulation.

13. ENTRY INTO FORCE AND TERMINATION

1. The provisions shall enter into force on the date of signature of both Parties.

2. Either Party may require the Provisions to be renegotiated if the legislative changes or inconsistencies in the Provisions so warrant.

3. The provisions apply as long as the service relating to the processing of personal data lasts. During this period, the provisions may not be terminated unless other provisions governing the provision of the service relating to the processing of personal data are agreed between the parties.

4. If the provision of the services relating to the processing of personal data ceases and the personal data has been erased or returned to the controller in accordance with Clause 11.1 and Annex C.4, the provisions may be terminated by either party's written notice.

5. Signatures

   On behalf of the AAU[2] (data controller)

   Place, date:

[2] This agreement is subject to electronic approval in Workzone by the legal person responsible at the AAU, i.e. the Head of Contract, ref. AAU Delegation Instructions.

Name:

Title: [Head of Institute/Titel on administrative responsibility, as specified in delegation instructions]

On behalf of the Data Processor

Place, date:

_____

Name:

Title: Project Manager [OBS: The signature shall be removed if it is an administrative agreement]

14. CONTACT PERSONS OF THE CONTROLLER AND THE PROCESSOR

1. The parties may contact each other via the contact persons below.

2. The Parties are obliged to keep each other informed of changes concerning contact persons on an ongoing basis.

DATA CONTROLLER:

Name	[NAVN]
Position	[STILLING]
Phone number	[TELEFONNUMMER]
E-mail	[E-MAIL]

THE DATA PROCESSOR:

Name	[NAVN]
Position	[STILLING]
Phone number	[TELEFONNUMMER]
E-mail	[E-MAIL]

ANNEX A INFORMATION ABOUT THE PROCESSING

A.1. The purpose of the processing of personal data by the processor on behalf of the controller;

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is to [CONTRIPTION. IN THE CASE OF SEVERAL PROCESSING OPERATIONS, THIS INFORMATION SHALL BE PROVIDED FOR EACH PROCESSING OPERATION;]

A.2. The processing of personal data by the processor on behalf of the controller is primarily concerned (the nature of the processing)

[DESCRIBE THE NATURE OF THE PROCESSING — F.EKS. ADMINISTRATION, RECORDING AND STORAGE OF PERSONAL DATA, OR ANALYSIS OF PERSONAL DATA FOR THE PURPOSES OF THE RESEARCH PROJECT]

A.3. The processing includes the following types of personal data concerning the data subjects

[DESCRIBE THE TYPE OF PERSONAL DATA PROCESSED, E.G.

General information: Social security number, name, email address, telephone number, address, personal identification number, payment card information, membership number, type of membership, attendance at gym and registration for specific fitness teams.

Sensitive Information: Health information

PLEASE NOTE: THE DESCRIPTION SHOULD BE AS SPECIFIC AS POSSIBLE.]

A.4. The processing includes the following categories of data subjects

[DESCRIBE THE CATEGORIES OF DATA SUBJECTS, E.G.

i. Interviewees in the research project
ii. Potential participants visiting the registration page for an event
iii. Invited persons to the controller's events
iv. Students enrolled at the Data Controller
v. Employees of the controller

A.5. Duration of the Agreement

[CHOOSE

The processing is valid until [SET ON THIS DATE OR REVISION TO the Main Agreement]

OR

The processing is not limited in time and is valid until the processor no longer processes Personal data on behalf of the controller. A description of the retention periods and the deletion mutines are set out in Annex C.4.

OR

The duration of the Data Processing Agreement follows the main agreement, [ANGIV REFERENCE TO the Main Agreement]. Termination of the main agreement for any reason will therefore also mean the termination of the Data Processing Agreement.]

ANNEX B SUB-PROCESSORS

B.1. Authorised sub-processors

Upon entry into force of the provisions, the controller has authorised the use of the following sub-processors

NAME	CVR	ADDRESS	DESCRIPTION OF TREATMENT

Upon entry into force of the provisions, the controller has authorised the use of the aforementioned sub-processors for the described processing operation. The Data Processor shall not, without the written consent of the Data Controller, make use of a Sub-Processor for a processing operation other than the described and agreed upon or make use of another Sub-Processor for this processing activity.

B.2. Notice for approval of sub-processors

The processor shall submit the request for a specific authorisation at least 4 weeks before the use of that sub-processor.

ANNEX C INSTRUCTIONS FOR THE PROCESSING OF PERSONAL DATA

C.1. Subject of treatment/instruction
The processing of personal data by the processor on behalf of the controller is carried out by the processor:

[INSERT DESCRIPTION FROM POINT A.2]

C.2. Safety of treatment
It is considered that the processor's processing activity on behalf of the controller is associated with low/medium/high risk, which is why a low/medium/high level of security must be established, cf. Article 32(1) of the Regulation.

In order to assess the level of safety, emphasis has been placed on the following assessment factors:

[THE CONTRACT ENTITY INSERTS POINTS FROM THE RISK ASSESSMENT TEMPLATE

FOR EXAMPLE:

- These are general personal data
- Data about 10,000 data subjects are processed
- The processing takes place solely in the systems of the controller;
- This is a short period from XX to XX

- It is a known processor in which the controller trusts]

The Data Processor shall then be entitled and obliged to make decisions on the technical and organisational security measures to be implemented in order to establish the necessary (and agreed) security level that adequately accommodates and manages that the processing is associated with [INSET security level low risk/medium risk/high risk].

[OBS: In the case of a data processor who is a student or is a small company that is unable to make decisions on security itself, then the minimum requirements for that processor as specified in the process for entering into data processing agreements shall be inserted instead].

C.3 Assistance to the controller
The Processor shall as far as possible — to the extent and extent set out below — assist the controller in accordance with Clauses 9.1 and 9.2 by implementing the following technical and organisational measures:

- The processor must have formal procedures for how assistance to the controller is handled within the company.
- The Data Processor shall ensure adequate internal procedures to enable the Data Processor to comply with its obligation to assist with security incidents, requests from the data subject and handling of data subjects' rights.
- The Data Processor does not answer or resolve a request from a data subject about his or her rights, including access, but forwards the request to the Data Controller as soon as the Data Processor is aware that it is the Data Controller who will process the request.
- The Data Processor shall also be able to inform the Data Controller within 4 hours of suspicion of a possible security incident.
- The processor shall record and document all correspondence with the controller relating to assistance to the controller.

C.4 Storage period/delete routine
See point 11.

C.5 Location of treatment
The processing of personal data covered by the Provisions may not be carried out without the prior written consent of the controller at premises other than the following:

[DATA PROCESSOR INDICATES WHERE THE PROCESSING TAKES PLACE]

[THE PROCESSOR SHALL ALSO INDICATE WHICH PROCESSOR OR SUB-PROCESSOR USES THE ADDRESS;]

C.6 Instructions for the transfer of personal data to third countries

[IF NO PERSONAL DATA ARE TO BE TRANSFERRED TO A THIRD COUNTRY, PLEASE INDICATE THE FOLLOWING:
"Data Processor is not entitled to transfer personal data to third countries within the framework of these provisions"]

[IF PERSONAL DATA ARE TO BE TRANSFERRED TO A THIRD COUNTRY, PLEASE SPECIFY THE BASIS FOR THE TRANSFER (FX CONSENT, STANDARD CONTRACTUAL CLAUSES).]

C.7 Procedures for the controller's audits, including inspections, with the processing of personal data entrusted to the processor

This agreement is assessed in accordance with the Danish Data Protection Agency's guidance on the supervision of data processors to obtain XX points. This means that the data processor must be supervised according to the following concept:

[CHOOSE CONCEPT — REMEMBER TO DELETE CONCEPTNUMMER

CONCEPT 1: It is agreed between the parties that as a rule there is no need to supervise the data processor.

OR

CONCEPT 2: It is agreed between the parties that the ata Processorshall of its own motion every 12 months, starting from the signature of the agreement, send a written confirmation that all requirements of the agreement are still being complied with.

Based on the results of the supervision, the controller is entitled to request the implementation of further measures to ensure compliance with the GDPR, data protection provisions of other Union or Member State law and these provisions.

OR

CONCEPT 3: It is agreed between the parties that the Data Processor shall, on its own initiative every 12 months starting from the signature of the Agreement;

1) send a written status on matters covered by the Provisions and other relevant areas (e.g. organisational or product changes); or

2) demonstrate in writing that the processing of personal data on behalf of the controller is carried out according to an updated certification, cf. Article 42 of the GDPR, or that the processor follows an approved code of conduct, cf. Article 40 of the GDPR.

Based on the results of the supervision, the controller is entitled to request the implementation of further measures to ensure compliance with the GDPR, data protection provisions of other Union or Member State law and these provisions.

OR

CONCEPT 4: It has been agreed between the parties that the processor shall obtain, once a year, starting from the signature of the agreement at its own expense, a statement of assurance from an independent third party regarding the data processor's compliance with the General Data Protection Regulation, the data protection provisions of other Union or Member States' national law and these provisions.

There is agreement between the parties that an ISAE 3000 auditor's declaration or equivalent auditor's declarations that may replace it shall be used in accordance with these provisions. The auditor's statement shall be transmitted to the controller for information without undue delay.

Based on the results of the supervision, the controller is entitled to request the implementation of further measures to ensure compliance with the GDPR, data protection provisions of other Union or Member State law and these provisions.

The controller or a representative of the controller has the right at any time to carry out exceptional supervision by the processor if the controller becomes aware of indications that it is necessary, for example, but not exhaustively listed, via press information, supervisory reports or own experience of security breaches.

In addition, the controller or a representative of the controller shall also have access to inspections, including physical inspections, with the premises from which the processor processes personal data, including physical premises and systems used for or in connection with the processing. Such inspections may be carried out when the controller deems it necessary.

C.8 [Delete, IF NO Sub-Processor] Procedures for audits, including inspections, with the processing of personal data entrusted to sub-processors

The Data Processor or a representative of the Data Processor is obliged to exercise adequate supervision of the Sub-Processor(s) in accordance with the Data Protection Agency's guidance for the supervision of processors and of its own motion to forward the results of these inspections to the controller no later than 7 working days after the inspection has been completed and any report prepared.

Any expenses incurred by the Data Processor and the Sub-Processor in connection with the supervision and preparation of reports shall be borne between the Data Processor and the Sub-Processor.

Based on the results of the supervision carried out by the processor, the controller is entitled to request the implementation of additional measures to ensure compliance with the GDPR, data protection provisions of other Union or Member State law and these provisions.

ANNEX D THE PARTIES' REGULATION OF OTHER MATTERS

D.1 Liability in relation to the data subjects
If a data subject claims compensation for material or non-material damage, Art. 82 GDPR applies.

D.2 Liability of the Parties
The parties are generally liable under the general rules of Danish law. Apart from material breach of the Data Processing Agreement, however, the Parties shall not be liable for indirect losses, consequential damages, operating losses, lost earnings or other financial consequential losses. For example, but not exhaustive, non-compliance with the instruction referred to in Section 3 is material non-compliance.

Except for intentional and grossly negligent acts and omissions, the Parties' mutual liability is limited in all respects to a total amount of DKK 500,000 per party.

The limitations of liability referred to above do not apply to recourse between the parties pursuant to Art. 82.