TU/e Atlas Living Lab Data Use Policy

Version 1.0, d.d. 8-01-2019
Workgroup Atlas Living Lab, Intelligent Lighting Institute TU/e

1. About this Data Use Policy

1.1. Introduction

This Data Use Policy is written by the TU/e Intelligent Lighting Institute. During its development from December 2017 to October 2018, this document has been discussed with and reviewed by the following TU/e bodies: the TU/e Union Counsel (Vakbondenraad), the Services Council (Dienstraad) the University Council (U-Raad), the faculty counsels of IE&IS and ID, and the task groups Atlas of IE&IS and ID.

1.2. Purpose and background

The purpose of this Data Use Policy is to outline the overall data management principles and practices devised to respect privacy and security of the TU/e campus community members (staff and students) and any other user of the Atlas building. This Data Use Policy is devised to meet the legal and ethical requirements as stated in the following documents: The General Data Protection Regulation (EU law 2018), The Netherlands Code of Conduct for Research Integrity (2018) and the TU/e Code of Scientific Conduct.

1.3. Scope and focus

This data use policy applies to all research and/or education projects that use the Atlas Living Lab facilities and technical infrastructure, which includes for example the luminaires, sensors, software and servers. This data use policy focuses on data use aspects of the projects in the Living Lab. The policy about experiments that involve physical interventions in a space with people, such as changes in light, temperature or other environmental conditions (human-subjects experiments) is covered in the VSNU and TU/e codes of scientific conduct mentioned in section 1.2. All human-subjects experiments in the Atlas Living Lab are bound to the conditions from these codes of conduct, alongside the conditions from this Data Use Policy.

1.4. Document outline

This document first describes the Atlas Living Lab goals and infrastructure, then treats the kind of data that can be gathered and then goes into the processes and facilities that are in place to treat the data responsibly. This Data Use Policy also refers to an Appendix with technical details that is accessible at www.tue.nl/atlaslivinglab [URL still to be confirmed].

2. About the Atlas Living Lab

2.1. What is a living lab?

A living Lab is a data-intensive infrastructure for scientific experiments on and observation of human subjects, coextensive with the everyday work and living environments of those subjects.

2.2. The Atlas Living Lab goal

Research and development of intelligent technologies and services for health, wellbeing and sustainability is an integral part of the TU/e and European research agenda. To tackle the challenges in these fields, researchers increasingly look into intelligent and networked technologies that are embedded in our built environment. Everyday life already shows a significant application of such technologies, with increasing impact on our lives and the environment. The long-term patterns of use and the effects on people, for example on health, wellbeing, social interaction and energy use, can only be researched meaningfully in the real, live world. A traditional lab environment cannot capture all the relevant complexities and long-term effects. To advance in these areas, a Living Lab environment is needed. The Atlas building offers a unique environment for research, with its large scale, its focus on sustainability, its place in the TU/e community, and its intelligent lighting infrastructure. The envisioned research domains span a broad range, including amongst others:

- Health: applying technology to promote vitality, well-being and prevention of disease and dysfunction.

- Intelligent Lighting: Effects of light on health, performance and well-being, e.g. prevention of Seasonal Affective Disorder and burn-out using personalised light exposure.
- Intelligent Lighting: Realising robust and effective artificial intelligence for indoor lighting applications.
- Energy: Study and influence environmentally relevant behaviour by means of, for example, energy saving applications and efficient facility management applications based on real-time insight in building usage patterns.
- Data Science: Gain insights from patterns in long-term building usage data.
- Persuasive applications and 'nudging' of behaviours by means of interactive technologies.

2.3. Description of the infrastructure

The Atlas Living Lab spans the 4th to 11th floor of the Atlas Building, excluding the toilets, technical spaces and emergency stairs. The Living Lab infrastructure is based on the Philips Connected Office lighting system. This basic infrastructure consists of the following elements:

- An IP based network infrastructure, part of the TU/e internal network
- Dimmable Philips LED luminaires that are IP addressable
- Sensors that capture information that in itself is anonymous and not uniquely identifying. The initial set of sensors is embedded in the luminaires and measures occurrence of movement (yes/no) in a range of approx. 2m by 3m for small movements (at a desk) and approx. 3m by 5m for large movements (walking).
- Control software: Philips Connected Office software allows monitoring of luminaires and sensors and control of dim levels of individual luminaires. The software also includes an Application Programming Interface, that allows other applications to read and control the hardware.
- The Atlas Living Lab server that extracts research data from the system and that runs applications made for projects in the Atlas Living Lab.
- The Atlas Research Database. This database stores data from the Atlas Living Lab.
- Information signs about Living Lab research at every entrance leading up to the Atlas Living Lab.
- The research infrastructure offers the possibility for including new sensors and controlling other building systems like heating.

3. Living Lab Data

3.1. What data is extracted?

Living Lab data includes all data that is generated in projects that use the Living Lab technical infrastructure. This includes both data that is extracted from the Connected Office system and data generated with ad-hoc data sources like questionnaires for an experiment. The appendix lists all data items that can be extracted from the Living Lab infrastructure. These data items include luminaire data, like dimming level or burning hours, and data from the occupancy sensors.
Data can only be gathered after a research proposal is approved by the TU/e ethical committee. See chapter 4 'Conditions for Living Lab use' for more details.
Note that the Connected Office system also generates internal data which is used specifically for its functioning. This data is not part of the Living Lab data: It does not enter the Atlas Living Lab research server and is not stored in the research database. Data from the Philips Personal Control App for mobile devices also does not enter the research server and is also not stored in the research data base.

3.2. Where can data be extracted?

Data from the basic infrastructure can be extracted from sensors that are distributed over floor 4 to 11. No sensors are present in the toilets, in technical spaces and in the emergency staircases.

3.3. Sensitivity of data

The data that can be extracted directly from the Living Lab infrastructure contains no direct personal identifiers. This means that no names, IP addresses, cell phone data, video feed, facial recognition, or any other kind of data that directly points to a person is generated. TU/e uses a rating to indicate different privacy aspects of the data using 'BIV': Beschikbaarheid, Integriteit, Vertrouwelijkheid. In English (and in reverse order) CIA: Confidentiality, Integrity and Availability. The possible scores on each of these elements are Low – Medium – High. The TU/e Chief Information Officer assesses the data that can be extracted from the Living Lab infrastructure as follows:

- Availability / Beschikbaarheid = High / Hoog,

- Integrity / Integriteit = High / Hoog,
- Confidentiality / Vertrouwelijkheid = Medium / Midden.

The level of confidentiality is related to how sensitive the data is (i.e., how much and what type of damage an individual would suffer if confidentiality was breached). Confidentiality is considered Medium. The data contains no direct personal identifiers, and contains no special personal data, such as a person's religion, race, political affinity, health or sexual orientation. But the usage patterns that can be extracted from the data could, in combination with other context information, possibly enable occupancy data to be associated to an individual. This is why provisions are taken to secure data, and why access to data is restricted and bound to conditions. These provisions and conditions are described in section 3.4 and chapter 4.

Note that the sensitivity analysis in this section only holds for the data that can be extracted directly from the Living Lab sensors and luminaires. In case a researcher wants to add other sensors or data sources, the researcher is required to perform a project specific sensitivity analysis, included in his or her research application.

3.4. Data storage and security

Living Lab data is stored securely in a data centre, used by TU/e, located in the Netherlands. The research data is retained for minimally 10 years, after which it could be deleted.

Considering the level of confidentiality (maximally 'Medium' category) the following technological and organisational precautions are taken to safely store the data:

- All data traffic between clients and servers is encrypted.
- Access to the Atlas Living Lab servers is exclusively granted from inside the TU/e network, using specific TU/e accounts assigned by the Labcoordinator. External parties that take part in an approved research project will receive temporary TU/e credentials to work from the TU/e network via a service like VPN.
- The Altas Living Lab servers are placed in a professional physical secure hosting environment, such as for example the NLDC.

4. Conditions for Living Lab use

4.1. Approval process

An important condition for use of the Atlas Living Lab for research is the approval of a research proposal by the TU/e ethical committee. This proposal includes a clear description of location and time-period, participants, ethical considerations and a Data Management Plan. In its judgement, the ethical committee upholds criteria such as "Avoidance of exploitation; Just distribution of benefits and burden; Respect for persons: Participants are treated as autonomous agents, Participants with diminished autonomy are entitled to protection; Respect for human dignity; Scientific validity; Scientific, social and/or educational relevance; Respect for rights and specific interests of (specific groups of) research participants, and/or the community/society" (from *Advies ethische toetsingscommissie mensgebonden onderzoek*, d.d. October 19th 2017). The research proposal should include informed consent from participants when required by the relevant codes of conduct and laws as stated in section 1.2. To assess practical feasibility, supporting services like Dienst Huisvesting and Dienst ICT could also be involved in the approval process.

Application is open to all research groups of TU/e. External parties like companies or institutes can enter the approval process under conditions. One condition is that the requested project fits in the Atlas Living Lab goals. Another condition is that there is a relation with TU/e research.

4.2. Opt-in / Opt-out

Part of the approval process mentioned in 4.1 is a check by the ethical committee whether required informed consent is provided. Only proposals that include the necessary informed consent will be eligible for execution. So, before an experiment can be conducted there is an opt-out or opt-in possibility for the relevant people. To offer an additional way to opt-out, 'Experiment-free' zones will be created when possible at the same floor as the experiment. In this way, people who want to opt-out will also have the possibility to work in such 'neutral' zones at the same (when possible) or another floor of the building.

4.3. Access to data by TU/e employees

The Living Lab data is shielded and not publicly accessible. The data is exclusively intended for academic purposes. Non-researchers have no access to the data, unless when required by law. Access is granted only after a research proposal is approved by the TU/e ethical committee. A Data Management Plan is part of the research proposal. This plan motivates what level of detail is needed in the data, how the data will be processed, if it will be combined with other data, how it will be stored and in what form it may be published. Access to data is mediated by the Labcoordinator, supported by the Data Steward. The Labcoordinator functions as a gate-keeper between the researcher and the data. The Labcoordinator makes sure only permitted data reaches the researcher in the right level of detail. Boundary conditions for access to the Living Lab data are that the researcher undertakes:

a. not to let the data form part of a publication;
b. only to show extensively abstracted and aggregated portions of the data;
c. to ensure that it is impossible under any circumstances for third parties to identify individual persons directly from the data;
d. to guard against the interests of TU/e or of any participant being harmed in any way whatsoever.
e. to use and gather data as sparingly as possible.
f. to exclusively use lawfully acquired data.
g. to inform the people involved of the data being gathered.
h. to use data exclusively for research, i.e. for the benefit of a publication, and ensure that no individuals can be recognized from the publication.
i. due care must be exercised in the amalgamation or enrichment of files that contain no personal data. Make sure that the new file will not yield a file with personal data.
j. data may not be transferred to a third party, external or internal to the TU/e. A separate research proposal must be approved for such data sharing.

In case the committee approves the application, the researcher receives access to the Atlas Living Lab server and gets permission to query and process the data under the provisions of the application.
Accessing already existing Atlas Living Lab data for new research must also be preceded by an approved research proposal, including evaluation by the TU/e ethical committee.

4.4. Access to data by external parties

An external party, such as for example another research institute, a company or a scientific journal may request access to data. An external party could be allowed access to research data only in case:

1. The party submits an Atlas Living Lab research application, including Research Data Management Plan, and it gets approved by the TU/e ethical committee. The boundary conditions for approval include at least those described in section 4.3 ‘Access to data by TU/e employees’.
2. The party additionally signs a Data Use Agreement that also addresses all points stated in section 4.3. This is a document with legal status that formalizes the Research Data Management Plan. Sanctions for non-compliance (‘boete clausule’) are optional in this agreement

Note: A request for data from a research journal can go directly to the approval committee.
Note: Research data is never sold to a third party. This means that no data is exchanged for money without the conditions and provisions set by TU/e, as described in this Data Use Policy.

4.5. Addition of sensors or other new data sources

- A researcher may want to temporarily use additional sensors or other data sources such as questionnaires for a specific experiment in the Atlas Living Lab, to complement the data from the Atlas Living Lab infrastructure. In that case, the implications on privacy are evaluated by the ethical committee and weighed in their decision to approve the proposal or not.
- Any new sensors or data sources that are to be added *structurally* to the Atlas Living Lab infrastructure can only be added after approval of the appropriate boards, including a representation of the building inhabitants. The application for the addition of sensors should include a Data Protection Impact Analysis (DPIA) to check, among other things, whether the plan is within boundaries of privacy legislation, if the security measures are sufficient and if transparency to the residents is sufficient.

5. Contact

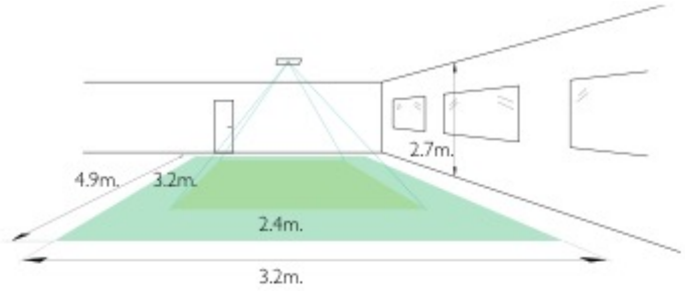
For questions and remarks about this privacy policy, please contact the management of Atlas Living Lab at atlaslivinglab@tue.nl. More information at www.tue.nl/atlaslivinglab.

Appendix

Last update 16-10-2018

Current sensors in the Atlas Living Lab infrastructure.

One Philips Actilume sensor is embedded in approximately every two luminaires. The Actilume sensor measures occurrence of movement (yes/no) in a range of approx. 2,4m by 3,2m for small movements (at a desk) and approx. 3,2m by 4,9m for large movements (walking). See the figure below. Sensors are present on the floors 4 to 11. No sensors are present in the toilets, technical spaces and above the emergency staircase.



Available data items from the Living Lab infrastructure

The following data items from the luminaires and sensors can be extracted from the Living Lab sensors and luminaires:

Data item	Comments
Device online status	Alarms like device not online
Energy consumption aggregated per area/floor/building and over time	Energy usage in Watts in a requested period
measured device temperature: max & min temp in period	Temperatures inside the luminaire, e.g, minTemperature = 20 degrees, maxTemperature = 40 degrees
module status	Alarms like ShortCircuitFault
Occupancy per individual device	Occupied percentage over a period, e.g. 50%. Unoccupied percentage over a period, e.g. 40%. Unknown percentage over a period, e.g. 10%. For periods of one minute, all percentages are either 0 or 100%
Occupancy aggregated per area/floor/building and over time	This is a percentage of the maximum possible occupancy over a time period
Alarms	Other alarms like LampOverLife
Timestamp	YY-MM-DD HH:MM:SS

The data that is extracted from the luminaires and sensors is stored with timestamp.