Security and Data Protection by Design and by Default for IoT Heat Pump Systems

Contribution to the IEA HPT TCP Annex 56

Task 1:
State of the Art

May 2023

Prepared by
Felix Schaber
Institute of Technology Assessment (ITA)
of the Austrian Academy of Sciences (ÖAW)

Table of Contents

1 Introduction

As the connectivity of heat pump systems increases, new applications and business models build around heat pump systems are developed. As many of these applications centre around data processing, it is important to consider information security and data protection while designing these systems.

The importance of information security is well known in this field. Whether in private homes or industrial settings, users are typically depended on their heat pumps to keep their homes warm or the industrial process going. However, the long technological lifecycle of heat pumps paired with the shorter lifetime of consumer electronics necessitated specific considerations for this field.

For example, technological standards widespread in the consumer market today may not remain available during the course of the heat pump lifecycle. The world of consumer electronics and household automation today is very different than it was 20 years ago. As technological and security standards evolve, it will be necessary to provide secure update mechanisms to swiftly update the systems while at the same time remaining easy to operate for users. This does also include planned deprecations of i.e. server infrastructure, so that users remain in control of their heat pump systems during the whole product lifecycle.

It is also important to consider that heat pump usage data reveal a lot about the environment it is used in. For example, in the residential setting, building occupancy can usually be derived by heating patters. This is valuable information worth protecting, as malicious actors like burglars or stalkers may abuse this information. Even if the systems use technical identifiers only meant to identify the heat pump, in the residential setting it is usually possible to identify the users behind the heat pump. Privacy is therefore an important topic for these systems. As privacy is a property of the overall system and not a feature of individual components, OEMs and suppliers need to work together with manufactures in order to achieve user privacy.

One important strategy to achieve this goal is privacy by design and by default, where privacy aspects are considered from the system design onset and without further user intervention and the most privacy friendly settings are chosen.

To assess the current practise of the industry, a survey among heat pump manufactures was performed during the course of this project. The results show that privacy by design and by default are considered important topics by manufactures when developing IoT heat pump systems. Despite their importance, manufactures only reported limited familiarity with these topics.

This document shall therefore provide guidance and recommendations specific to heat pump systems. After a brief overview of the essential concepts of information security and data protection, the focus of these document is on questions of particular relevance for IoT heat pump systems.

2 Information Security

Information security deals with the protection of information in systems. Its purpose is the “preservation of confidentiality, integrity and availability of information”.[1] Confidentiality means that only authorized parties have access to the information and information is not disclosed to unauthorized parties. Integrity means that the information has not been

[1] ISO/IEC 27000:2009

modified. And lastly availability implies that the information can be accessed by authorized parties when needed.

2.1 Available materials

Many recommendations and guidelines for security of IoT devices are available from different organizations, i.e. the baseline security recommendations for IoT[2] by ENISA or the Cyber Security for IoT: Baseline Requirements[3] from ETSI. There are also guidelines which combine security and privacy like ISO/IEC 27400:2022 IoT security and privacy guideline.[4] They are mostly focused on general advice applicable to a wide range of IoT devices. The focus of this document shall therefore be on topics arising from the specific characteristics of IoT heat pump systems.

2.2 Current developments

Many data protection norms also contain provisions for information security. However, if data protection norms are not applicable for a specific system, there currently is little regulation on information security from a legal perspective. Note that this may change in the future with the current proposal for the e-privacy directive, where machine to machine communications only concerning legal persons may be regulated as well.[5] However, the discussion process on the e-privacy regulation has long been ongoing and it is currently[6] unclear when and with what provisions the regulation will be finalized. Similarly, the proposed European Cyber Resilience Act directly targets the security of IoT products, but is still under discussion.[7]

Note however that for consumer products additional stipulation for security already exist as part of the product warranty requirements.[8] This also includes the requirement to make security updates available.[9]

3 Data Protection

In contrast to information security, the purpose of data protection is to guard fundamental rights and freedoms of natural persons with regards to their privacy.[10] Many provisions of data protection revolve around the concept of personal data. The General Data Protection Regulation[11] (GDPR) defines personal data as “any information relating to an identified or identifiable natural person (‘data subject’) […]”.[12] The GDPR is only applicable if personal data is processed.

---

[2] https://web.archive.org/web/20230312044622/https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/

[3] https://web.archive.org/web/20220829150324/https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf

[4] https://web.archive.org/web/20230313072008/https://www.iso.org/standard/44373.html

[5] Proposal for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

[6] As of march 2023

[7] Proposal for a Regulation of the European Parliament and the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

[8] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC

[9] See Art 7 (3) and Art 10 (2) Directive (EU) 2019/771

[10] Art 1 (2) GDPR

[11] 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 (General Data Protection Regulation)

[12] Art 4 (1) GDPR

3.1 Personal data

One key question for IoT systems is therefore if personal data is being processed. It is important to note that it the concrete identity of the natural person does not need to be known, it is sufficient that the person can be identified. This implies that identifiers which can be reconnected to a natural person (i.e. pseudonymous data) are considered personal data for the purpose of the GDPR. The GDPR does not protect the privacy of legal persons (i.e. companies).

There is an important distinction between domestic and industrial installations. While information security principles should always be applied, the applicability of data protection is bound to the processing of personal data.[13] This is much more likely in domestic/residential settings where a single household is using the IoT heat pump, than in a commercial setting, where heat pumps are used part of commercial offering or an industrial process. Heat pump usage data in the residential setting may reveal building occupancy and therefore clearly affects user privacy and can easily be abused (i.e. by buglers or stalkers). At the same time, it is important the right users remain in control of the heat pump system. Otherwise after an ownership change, former building occupants may remain in control of the heat pump without the new occupant's awareness.

However, if it is unclear whether the IoT heat pump system is used in a consumer or industrial setting, it is recommended to assume personal data is being processed.

3.2 Controllers and Processors

Another important distinction is between data controllers and data processors. Controllers determine the "means and purposes of the processing of personal data"[14] while processors "process personal data on behalf of the controller".[15] The distinction is important because many data protection obligations apply directly to controllers. The controllers are then in turn responsible for ensuring the processors meet the requirements set out by the GDPR.[16] This can be achieved by contractual agreements between data controller and processor. Standard contractual clauses approved by the European Commission[17] are often used for this purpose.[18]

An example for a processor would be an external cloud, providing storage and computing power used by an OEM to analyse personal data collected from an IoT heat pump system. Note however, that multiple controllers can be involved in the same data processing activity.

For example, if the external cloud provides an analysis platform where not all processing purposes are decided upon by the OEM, the cloud provider would become a joint controller together with the OEM. While joint controllers may have an agreement how the responsibilities are distributed,[19] data subjects still may choose which controller to address when exercising their rights under the GDPR.[20] The European Data Protection Board (EDPB)

---

[13] For further information see the section on data protection
[14] Art 4 (7) GDPR
[15] Art 4 (8) GDPR
[16] Art 28 (1) GDPR
[17] https://web.archive.org/web/20230313072101/https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en
[18] Note however that these contractual clauses have been updated in 2021 by the European Commission after a decision by the European Court of Justice. Older data processing contracts may therefore require an update in order to stay GDPR compliant.
[19] Art 26 (1) GDPR
[20] Art 26 (3) GDPR

Guideline 07/2020 offers additional information on the concepts of data controller and processor.[21]

3.3 Rights of the Data Subjects

The data subject enjoys multiple rights under the GDPR. Among others these include the right of access to the stored personal data,[22,23] the right to rectify inaccurate personal data,[24] the right to data portability,[25] as well as the right to demand the erasure of personal data or restrict its processing under certain conditions.[26] In addition, the data subject shall also be provided with a range of information when personal data are obtained.[27] These data subject rights apply to processing of personal data in general and are not specific for IoT systems.

3.4 Principles

The GDPR contains multiple principles when processing personal data.

The processing must be lawful and for an explicit purpose.[28] Of particular relevance is the principle of data minimization, which states that the purpose of any data processing shall be "adequate, relevant and limited to what is necessary" for the specified purpose.[29] In addition the data shall only be stored as long as necessary for the specified purpose and be kept up to date in order to remain accurate.[30] The GDPR also contains responsibilities from the information security perspective, namely that integrity and confidentiality of the processed data shall be maintained.[31] The controller is responsible for demonstrating compliance with these principles.[32]

The definition of a data processing purpose is therefore essential when designing IoT Systems, as compliance with many these principles is only possible relative to a given purpose. In addition, the more concrete the stated purpose is, the easier it is to follow the principles of privacy by design and privacy by default, as these principles require knowledge about the required information and processing steps of specific applications.

3.5 Lawfulness of Processing

In addition, the GDPR also requires a legal basis for each of the processing purposes. In the private sector, controllers often use consent, processing which is necessary for a contract or legitimate interest as legal basis.[33] Each of these legal bases carries their own requirements.

Consent is often used as a legal basis but requires careful management by the controller. First, the burden of prove that the data subject has in fact given consent rests with the controller.[34] The data subject must be informed of the right to withdraw consent at any point in the future, after which future processing for this purpose must be stopped. Second, data subjects may consent to specific purposes only, while not giving consent for other processing

[21] https://web.archive.org/web/20230226212620/https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf
[22] Art 15 GDPR
[23] See the EDPB guideline 01/2022 for further guidance on the right to access: https://web.archive.org/web/20230313072418/https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en
[24] Art 16 GDPR
[25] Art 20 GDPR
[26] Art 17 and 18 GDPR
[27] Art 13 and 14 GDPR, this is often done by a privacy notice
[28] Art 5 (1) (a) and (b) GDPR
[29] Art 5 (1) (c) GDPR
[30] Art 5 (1) (d) (e) GDPR
[31] Art 5 (1) (f) GDPR
[32] Art 5 (2) GDPR
[33] Art 6 (1) (a) to (c) and (f) GDPR
[34] Art 7 (1) ARt

purposes. The separate consent must be possible for each purpose and the purpose must be described “using clear and plain language”.[35] Third, the consent must be freely given not i.e. taken as precondition in order to obtain another service. If this other service could also be performed without processing the data, then the consent is usually not considered to be freely given. If at least one of these conditions is not fulfilled, using another legal basis may be appropriate.

If the processing is strictly necessary in order to fulfil a contract, then it usually preferable to use this instead of consent as a legal basis. For an IoT heat pump system, this could for example be maintenance contract requiring the technician to access to the heat pumps data in order to perform maintenance. Note however that this is limited to what is strictly necessary for contract performance. If for example no maintenance contract is active for a specific heat pump system, then under this legal basis maintenance data may not be collected from this system in order to ease possible future onboarding.

Another legal basis is legitimate interest for a specific processing purpose. In this case, the controller must additionally demonstrate that the given interests outweigh possibly conflicting interests of the data subjects. For this, a balancing test is usually performed and documented. Only if the balancing tests shows a positive result this legal basis may be used. For IoT heat pump systems, this could for example include system monitoring to prevent unsafe and potentially hazardous operating conditions or the prevention of cybersecurity risks.

3.6 Privacy by Design

Data protection principles are most effective when they are incorporated early into the product lifecycle. The GDPR therefore requires controllers consider these principles already during the design phase of a product, where the means of processing are determined.[36] Note that this applies for all data protection principles and may require measures beyond pseudonymization.[37]

These protections shall be implemented by appropriate technical and organizational measures. A risk-based approach is used to determine which measures are appropriate given the concrete application. The risk is determined by considering the severity and likelihood of threats caused by the processing to the privacy of natural persons. At the same time the “state of the art, the cost of implementation and the nature, scope, context and purposes of processing”[38] shall be considered for this as well.

For example, a heat pump used for residential heating is also essential for comfort within the building. Loss of operation may therefore critically affect users, especially during the winter months. The extend of risk strongly depends on the way the IoT heat pump operates. If the heat pump can be controlled over the internet likelihood of this threat will be much higher than if control is only possible over the local network. Similarly, the severity will depend on the degree of control an attacker may obtain over the IoT heat pump system. If physical damage to the heat pump system is possible, the severity will be much higher than a simple increase or reduction of building temperature.

When used in a residential setting, an IoT heat pump may also provide information about building occupancy. The information can be considered personal data, even if the information is only collected on a household level. It may pose a threat if abused (i.e. by buglers,

[35] Leg cit
[36] Art 25 (1) GDPR
[37] Data minimization and pseudonymization are listed as possible measures in Art 25 GDPR. However, they only servers as examples and shall not be regarded as exhaustive list.
[38] Art 25 (1) GDPR

stalkers, etc.). Again, the risk of this threat depends on degree and extend of information accessed (accessible). Note that this considers not only external attackers but also the availability of the information within the organization or authorized external partners. The intent of privacy by design is therefore to combine technical with organizational measures in order to achieve system wide safeguards for privacy.

An important characteristic of heat pump systems is their long lifespan, which can be over 20 years.[39] It is important to consider technological changes for users as well as suppliers during that lifetime. The technological lifecycle of user devices is usually much shorter than for commercial applications. For example, 20 years ago today's most widely used mobile operating systems[40] did not exist. The field of smart home standards is also developing, where many systems are currently based on vendor specific solutions,[41] while vendor neutral solutions[42] are gaining ground.

Considering the long lifespan of heat pump systems, it is highly likely that changes both technological and security standards will occur over the systems lifetime. The GDPR therefore requires that the analysis is not only valid during system design but also when the data processing is actually performed.[43]

Another issue arising from the residential setting in combination with the long lifetime of IoT heat pump is ownership change. When the occupants of the household change, it should not be possible for the old users to monitor and control the heat pump of the new users. Likewise, the new user should not gain access to the occupancy data of the old user. The IoT heat pump should therefore provide a mechanism to delete usage data and disconnect the old users account from the heat pump. In addition, the new user should be able to connect their device without further interaction with the old user, i.e. by using a pairing procedure. Even though the heat pump system stays the same, it collects data from different people, which are supposed to be secured by privacy norms.

A precise processing purpose can also provide valuable guidance when implementing privacy by design. Implementing data minimization is much easier if the exact amount and granularity of data required is evident for each purpose. For example, if it is known a maintenance technician only requires time averaged values from certain components for diagnosis, only storing these time averaged values may help data minimization while at the same time speeding up the diagnosis process.

In addition, if the entire process, from data collection over storage and computation up to deprecation and deletion, is considered, it becomes much easier to determine who needs to access the data when and for what reason. This also helps to protect data confidentiality, may additionally facilitate the purpose limitation principle and guide appropriate policies for storage limitation.

When designing interfaces and applications for these systems, it is therefore important to keep technological obsolescence in mind and use connectivity standards and platforms which are likely to remain available during the lifetime of the IoT heat pump system. In some cases, it may also be possible to provide software updates allowing older systems to become compatible with newly developed standards. However, it is often beneficial for both users and manufactures to use long lived standards. That way privacy by design can also benefit system design.

[39] European Heat Pump Association, European Heat Pump Market and Statistics Report 2019
[40] As of the time of this writing, these are Android and iOS
[41] At the time of this writing examples include Apple Home Kit, Samsung smartThings, etc.
[42] i.e. matter and thread
[43] Art 25 (1) GDPR

3.7 Privacy by Default

Privacy by default is again closely connected with the processing purpose. In essence, it states that the default system settings should limit data processing to the absolute minimum necessary in order to perform the specific purposes.[44] Specifically, this implies without further user interaction, data processing will remain minimal. Besides data collection, this applies to storage, computing and data access as well.[45]

Importantly, this provision applies to the data processing system as a whole and is not limited to the parts supplied by the controller. For IoT heat pump systems, this implies that a manufacturer may need to assess all system components for data protection settings. This includes i.e. parts supplied by different vendors or third-party software or services for data analytics.

General information on this privacy by default and by design can also be found in the EDPB guidelines.[46]

3.8 Security of Processing

The GDPR also contains provision regarding the security of processing. As for privacy by design, it is based on a risk-based approach that shall take the “state of the art, the costs of implementation and the nature, scope, context and purposes of processing”[47] into account. The phrasing suggests the test is to be performed in a similar manner than for privacy by default.

In also contains exemplary list of possible measures, including pseudonymization and encryption as well as confidentiality, integrity, availability and resilience of the systems.[48] These properties need to be ensured for the system as a whole and are not limited to specific parts of the system.

Especially availability and reliability are critical for essential utilities such as heat pump systems. The heat pump should therefore continue to function even if the internet connectivity is lost. In the event of connectivity loss, the heat pump should remain available, using a graceful degradation mode where all functions not requiring connectivity remain available. Likewise, control of the heat control of basic heat pump functions shall always be possible by the user. This can be achieved by e.g. using a panel directly controlling the heat pump. Similarly, the essential operational features of a heat pump should be always accessible independent of any server connection.

The taken measures shall also be regularly tested and evaluated.[49] From the supplier side, this may imply a need to support and update the technological infrastructure for the IoT heat pump systems. This is especially relevant if the IoT heat pump can be monitored or controlled externally, as the information security standards and protocols are likely to change during the long lifetime of the system. This also necessitates the need for a secure update mechanism, as it is likely impossible to predict all necessary changes ahead of time. Otherwise, the IoT heat pump may become vulnerable to cyberattacks, e.g. by holding the heat pump function for ransom until a payment is made.

Another potential security hazard is the integration of the IoT heat pump into the home automation system. Such networks may contain insecure devices which may be

[44] Art 25 (2) GDPR
[45] Leg cit
[46] See European Data Protection Bord, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, adopted 20.10.2020
[47] Art 32 (1) GDPR
[48] Art 32 (1) (a) and (b) GDPR
[49] Art 32 (1) (d) GDPR

compromised and provide a launch pad for attackers into the local network. Protection of IoT heat pump against cybersecurity hazards is therefore not only needed against attacks from the internet but also from within the local network.

4 Conclusion

In summary, it is important to consider the specific characteristics of IoT heat pumps when implementing privacy by design and by default. Due to both the long lifecycle as well as the systems importance for building comfort and user privacy it is paramount to take a long-term perspective.

Technological and security standards may change, while the IoT heat pump system shall remain reliable and available and data protection shall be upheld thorough the systems lifetime. To that end, it is important to build on technologies which can be expected to remain available during the systems lifetime, both at the end users and the supplier's side, while also providing the possibility for frictionless security updates of the system. Data protection and security should not be evaluated once but regularly during the lifetime of the project to ensure that the assessment remains up to date.

Data protection and security are not only technical procedures but a property of the system as a whole. It needs to include organisational as well as technical measures. Therefore, external suppliers, third-party software as well as internal procedures used for data processing also have to be evaluated. Only when the whole system lifecycle is considered, privacy by design can show its true potential in both guiding and aiding the system development.

5 FAQ

Am I processing personal data when I don't know the identity of the heat pump user?

The general data protection regulation (GDPR) does not require that the specific user is identified. It is sufficient that the user is identifiable by using reasonable means. This implies that a pseudonymous identifier (i.e. a device ID) can be personal data as well, if the identity of the user can be inferred by cross-reference with another database available to the controller.

True anonymization of fine granular data can be difficult. If in doubt, it is therefore recommended to assume personal data is being processed and to apply the data protection norms accordingly.

As a heat pump OEM, do these provisions apply to me?

Whether data protection norms apply directly depends on if you decide the means and purposes of the data processing. If this is the case then you are considered a data controller and directly responsible to show that the GDPR provisions are implemented for the system. Otherwise, the means and purposes are decided elsewhere, you may be considered a data processor.

However, the GDPR requires controllers to ensure that processors uphold data protection principles when processing personal data. It is therefore highly likely the norms will still apply indirectly, as downstream controllers will most likely require data protection principles on a contractual basis. Even if acting as a processor, knowledge of GDPR principles is therefore essential.

As a heat pump manufacturer, do I need to monitor my suppliers for data protection?

If you decide the means and purposes of the processing of personal data, then you will need to ensure your suppliers uphold the GDPR principles as well. Note that this also includes additional processing performed by the suppliers and default settings deciding which data processing is performed.

For further information, please refer to the section controllers and processors of this document.

In order to show the security of processing personal data, is it sufficient to fulfil the relevant security norms and standards?

Norms, standards, certifications and codes of conduct can help to show that the security of processing is upheld. As such it is usually a good idea to follow them during system design and implementation, and document their application.

However, codes of conduct need to fulfil the criteria of Art 40 GDPR and certifications of Art 42 GDPR for official recognition. In all other cases, the compliance with the security of processing under GDPR will need to be assessed and documented separately.