GDPR

3DE

1220514 – Liam Saliën

1220528 – Juuso Jalava

1220379 – Benjamin Moreira

1220459 – Patryk Pas

1220448 – Miika Kauppinen

Contents

[1. Introduction 3](#_Toc123573467)

[2. Contact 3](#_Toc123573468)

[3. Processing of Personal Data 3](#_Toc123573469)

[What 3](#_Toc123573470)

[The information we collect 3](#_Toc123573471)

[Where + our intentions 3](#_Toc123573472)

[Legal base 3](#_Toc123573473)

[Legitimate interest 4](#_Toc123573474)

[Retention period 4](#_Toc123573475)

[4. Your User Rights 4](#_Toc123573476)

[- **The right to be informed:** 4](#_Toc123573477)

[- **The right of access:** 4](#_Toc123573478)

[- **The right of rectification:** 4](#_Toc123573479)

[- **The right to be forgotten:** 5](#_Toc123573480)

[- **The right to restrict processing:** 5](#_Toc123573481)

[- **The right to data portability:** 5](#_Toc123573482)

[- **The right to object:** 5](#_Toc123573483)

[5. Data Security 5](#_Toc123573484)

[6. Data Breaches 5](#_Toc123573485)

[7. Conclusion 6](#_Toc123573486)

[8. Sources 7](#_Toc123573487)

# 1. Introduction

The General Data Protection Regulation (GDPR) is a tough privacy and security law that imposes obligations onto organisations (anywhere in the world), so long as they target or collect data related to people in the EU.

This report is made in accordance with the GDPR, so that users know their rights and which personal data is being processed by us, ElectricGo. It also covers Data Retention policies and Data Breaches.

# 2. Contact

All questions regarding privacy, or general questions about your rights and more, can be asked at [privacy@electricgo.com](mailto:privacy@electricgo.com).

For personal and sensitive questions, it is possible to contact our *Data Protection Officer* (Benjamin Moreira) at [benmorprivacy@electricgo.com](mailto:benmorprivacy@electricgo.com).

# 3. Processing of Personal Data

## What

Personal Data is *all* the information relating to an identified or identifiable natural person, as defined in *Article 6 of the GDPR*.

Under processing of Personal Data we understand all the operations that are operated on Personal Data. Those include, but are not restricted to collection, recording, storing, alterations, retrieval, restriction, erasure, etc. etc.

## The information we collect

To serve its purposes, and provide its services, ElectricGo is processing the following data:

* First name
* Last name
* Email
* Phone number

## Where + our intentions

The processing of this data is done in both Portugal and Germany, and is only retrieved by us, ElectricGo. We will never sell or transfer this data to other parties outside of our company, and also have no intentions to transfer it to other countries except Portugal and Germany.

## Legal base (Art. 6)

The processing of your personal data is covered by the legal basis of the GDPR that includes both **contract** and **legitimate interests**.

## Contract

As described in the GDPR, this means: “When the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract”.

All employees of ElectricGo are party to a contract, as you signed and agreed with our terms when starting at the company. This work agreement/contract allows us to process your personal data to fulfill the terms of this contract, as we need to be able to identify every single employee in our company.

## Legitimate interest

This is defined as “when processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”.

In our case this means that we need to use employee data for certain purposes.

As a company that wants to have a secure application, we have the legitimate interest to verify and identify all the users/employees of our platform, for which the requested data is necessary. We don’t intend to use this data for anything else.

When processing your personal data, ElectricGo guarantees you, the user of the ElectricGo application, that the following GDPR principles are being respected and followed (Art. 5):

* Loyalty: your data is being treated in a lawful manner.
* Purpose: your data is collected for identification and verification purposes and not further processed in a manner that is incompatible with those purposes.
* Data minimization: we only ask and store what is really necessary and relevant for our identification purposes. We guarantee that no irrelevant data is being collected.
* Accuracy: the data should be accurate and be kept up to date. Users have the right for modification and alteration of their data (see 4. User Rights).
* Storage Limitation: the data will be stored no longer than is necessary for the purposes for which the personal data are processed, and will be erased as soon as the user demands to be anonymized and the data to be deleted.

## Retention period

ElectricGo guarantees that the personal data will be stored as long as the user is using the application and doesn’t require to be anonymized, as this data is necessary for the identification.

The users have the right all the time to demand anonymization or deletion of their data, unless it is not allowed because of lawful restrictions and reasons. This means that ElectricGo won’t use data no longer as needed, and will immediately erase all traces of your data when requested to.

# 4. Your User Rights

The GDPR provides the following data rights for EU individuals and users of the ElectricGo Application:

## **The right to be informed (art. 13):**

Please take a look at [3. Processing of Personal Data.](#_3._Processing_of)

## **The right of access (art. 15):**

As an employee you have the right to request your personal data at [privacy@electricgo.com](mailto:privacy@electricgo.com), free of charge. We will respond within maximum a month with a copy of your data in a machine readable format.

## **The right of rectification (art. 16):**

You as an employee has the right to rectify inaccurate information, or to complete incomplete information. You can request this at [privacy@electricgo.com](mailto:privacy@electricgo.com), please include “Rectification” in the title, and we will respond within a month.

## **The right to be forgotten (art. 17):**

You have the right to withdraw your consent about us processing your Personal Data by requesting us to erase your data/to be forgotten. This can be done by sending a request to [privacy@electricgo.com](mailto:privacy@electricgo.com), please include “Erasure” in the title. We will respond to you within a month.

Note that this can only be done when you’re not an employee of ElectricGo anymore.

# 5. Data Security (art. 32)

In order to guarantee the confidentiality, integrity and availability of the data collected, the latter can only be consulted, edited and modified by an administrator authenticated as such. For this, an authentication system has been set up to guarantee the identity of each user, and to make certain critical actions available or not depending on the type of user.

Moreover, in order to guarantee the confidentiality of passwords, they are stored in the form of a hash and pass through a communication tunnel encrypted using the TLS/SSL protocol, which can be identified by the padlock in the URL bar.

Finally, ElectricGo commits to periodic backups of its users' personal data on physically separate servers in order to be more responsive in the event of a data breach and to always be able to meet the privacy needs of its users.

# 6. Data Breaches (art. 33)

Despite all the care taken to ensure the security of our users' personal data, it can happen that data leaks occur.

When this happens, we are committed to keeping the relevant local supervisory authorities informed. Depending on the severity of the leak, we may inform users of the existence of the leak, as well as the nature of the information involved.

To prevent data leaks, we have several tools in place. On the one hand, our servers are equipped with firewalls that prevent intrusions and record all activity related to the access of machines and their resources. In addition, our servers are equipped with systems that protect them from brute-force attacks by ignoring repeated requests to our services. Any intrusion will be reported to us by email as soon as it is detected. Moreover, for legal and security reasons, we register all access to our service and the source ip address in a log file. Finally, every activity on the servers is registered into log files for some amount of time.

In the event of a data leak, we will follow the following plan:

* Identification and assessment of the severity of the leak:

In order to identify the extent of the damage, we will identify the nature of the leaked data (names, passwords, phone numbers, decryption keys, etc.) as well as the quantity leaked and, in the case of data deletion, the presence of a backup or not. Based on these three parameters, we will be able to evaluate the severity of the leak. In order to identify the nature of the leaked information, we will link the log files, periodically saved on a physically separate server.

* Notification of the relevant authorities and individuals in a timely manner:

We will notify the appropriate local data protection authorities and, if the leak represents a high risk to users, then we will inform users of the nature of the leaked data through an email.

* Determination of the origin of the leak and identification of areas for improvement:

In order to determine the origin of the leak, we will link the log files of the servers in order to extract information that can give clues on the source of the incident (such as the IP or Mac address for example). By knowing the source of the incident, we will then be able to determine which security system failed to protect the server(s) from the attack and thus improve the security of our users' personal data.

* Prevention of future incidents:

Once the above improvements have been determined, ElectricGo is committed to implementing them and thereby ensuring a higher level of security for our users' personal data.

# 7. Conclusion

For reasons of security, legality and reliability, ElectricGo must process certain personal data of its users. However, ElectricGo is committed to processing this data in a clear, transparent and purposeful manner. Indeed, the privacy of our users is very important to us. That's why ElectricGo only processes data that is truly necessary, and for the shortest period of time possible. However, should a leak occur despite our efforts, ElectricGo will inform the parties involved and identify the extent of the leak, so that we can always provide the highest level of security to our users.

# 8. Sources

GDPR individual data rights and access, 29 July 2020, <https://www.gdpreu.org/the-regulation/list-of-data-rights/right-of-access/>

The Eight User Rights Under the GDPR, Nicole Olsen, 01 July 2022, <https://www.privacypolicies.com/blog/gdpr-eight-user-rights/#How_To_Create_A_Gdpr_Compliant_Privacy_Policy>

LAPR5 : Skill Module, Law and Ethics, Francisco Marques Vieira, 27 October 2022, <https://moodle.isep.ipp.pt/pluginfile.php/259220/mod_resource/content/1/2022%20ISEP%20LAPR5%20aulas%20RGPD%20EN.pdf>