Brilliant

# Brilliant Internal Privacy Policy

2024-10-24
Version 1.3
Classification: Public

## Versions

| Version | Author | Approved by | Date | Description |
|---|---|---|---|---|
| 1.0 | Erik Ålander, Delphi | Johan Pellbäck, CTO Ulrika Jonsson, CEO | 2024-10-21 | First draft |
| 1.1 | Johan Pellbäck | Ulrika Jonsson, CEO | 2024-10-22 | Complementary process documents and references |
| 1.2 | Erik Ålander, Delphi | Ulrika Jonsson, CEO | 2024-10-23 | Complementary information chapter 5 |
| 1.3 | Johan Pellbäck | Ulrika Jonsson, CEO | 2024-10-24 | New template |
| 1.4 | Johan Pellbäck | Ulrika Frimmel, CEO | 2026-01-07 | Update references in chapter 9 |

Brilliant

**TABLE OF CONTENTS**

Brilliant

## Purpose and background

The purpose of this Privacy Policy is to clarify and establish Brilliant Future AB's (”Brilliant Future”) approach to the processing of personal data and to provide practical guidance on how personal data should be processed within Brilliant Future.

This privacy policy contains general guidelines for how personal data should be processed within Brilliant Future, regardless of whether the processing is carried out by Brilliant Future or by a third party on behalf of Brilliant Future. The privacy policy is divided into two parts, a general part that describes the legal background and measures and assessments needed before processing personal data and a practical part that describes practical measures that need to be taken when processing personal data.

Brilliant

## PART I - LEGAL BACKGROUND

### 1. Definitions

1.1 In this Privacy Policy, the following words, whether used in the plural or singular or in the definite or indefinite form, shall have the meaning indicated below when the first letter is capitalized:

**Processing:** means any operation or set of operations which is performed on Personal Data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

**Data Protection Rules:** means the law or regulation in force from time to time applicable to the Processing of Personal Data, including but not limited to the GDPR; and the binding decisions and regulations of IMY and any subsequent local adaptation and regulation regarding data protection;

**IMY**: the Swedish Authority for Privacy Protection;

**GDPR**: 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);

**Sensitive Personal Data**: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data and data concerning health, sexual orientation and sex life, as described in Article 9 of the GDPR;

**Controller:** means a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;

**Processor**: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller;

**Personal Data Breach**: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

**Personal Data**: means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or

more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

**Data subject**: an identified or identifiable natural person to whom the Personal Data can be related.

## 2. Legal and regulatory framework applicable to the Processing of Personal Data

2.1 The GDPR entered into force on 25 May 2018 and has direct effect in Sweden and in all other EU countries. This privacy policy is based on the GDPR as well as guidance and national legislation that complements the GDPR.

## 3. Data Controller and Data Processor

3.1 Personal Data can be Processed by Brilliant Future in two different roles, either as a Data Controller or as a Data Processor. When Brilliant Future decides why (the purpose) and how (the means) Personal Data is to be Processed, Brilliant Future is to be considered as the Data Controller and thus obliged to ensure that the Processing of Personal Data is done in accordance with the GDPR.

3.2 If Brilliant Future Processes Personal Data on behalf of someone else, Brilliant Future is considered a Processor. When Brilliant Future is a Processor, the main task is to Process Personal Data only on the documented instructions of the Controller and to fulfil the requirements set out in Article 28 of the GDPR. These requirements must be regulated in a contract, known as a Data Processing Agreement. Article 28 of the GDPR states that a Processor shall, inter alia:

- Take appropriate technical and organisational measures.
- Appropriate confidentiality/secrecy obligations for employees working with Personal Data on behalf of the Controller.
- Assisting the Controller in the fulfilment of the Data subject's rights.
- Only use sub-processors authorised by the Controller (either through a general consent or explicit consents in each case).
- Delete or return Personal Data at the end of the contractual relationship.

## 4. Purposes and legal basis of the Processing

4.1 The Controller may only collect Personal Data for specified, explicit and legitimate purposes. This means that the Processor must know the purpose of the Processing even before the collection of Personal Data begins. The Personal Data must not be Processed in a way that is incompatible with the original

purposes. In other words, the predetermined purposes are what sets the framework for the Processing. The purposes should be documented in writing and the Data Subject should be informed of the purposes both when the data is collected and otherwise when requested. If the Personal Data collected are later to be Processed for purposes other than those compatible with the original purposes, the Data Subject must also be informed of this.

4.2 In order to be allowed to Process Personal Data, there must always be support in the GDPR, a so-called legal basis. Relevant legal bases for Processing Personal Data for Brilliant Future under the GDPR are:

1. Consent of the data subject,
2. The Processing of Personal Data is necessary:
    a. to fulfil a contract with the Data Subject,
    b. to fulfil a legal obligation, and
    c. after a balancing of interests.

Different rules apply to Sensitive Personal Data and data relating to criminal offences. For Sensitive Personal Data, see section 7.

4.3 The Controller must ensure that Personal Data are only Processed for legitimate purposes and that there is a legal basis for any Processing carried out. It must also ensure that information about the Processing is provided to Data Subjects.

4.4 When consent is used as a legal basis, it is required to be freely given, specific, informed and unambiguous. It is therefore important that in situations where consent is used as a legal basis, it is clear what the consent is for, and that information is available when consent is obtained. Where consent is obtained by automated means, this can ideally be done through a link to a relevant information/privacy policy together with the consent text that the Data Subject agrees to by ticking a box (the box must not be pre-ticked).

## 5. International aspects

5.1 It is the responsibility of the Controller to ensure that Personal Data transferred outside the EU/EEA always fulfils one of the following conditions in the receiving country (even if such a transfer is made by a Processor):

1. There is a decision by the European Commission that, for example, a certain non-EU/EEA country ensures the so-called adequate level of protection,
2. Contracts containing the European Commission's model clauses (2010/87/EU) have been concluded, without any changes or additions that contradict the clauses,

3. Binding Corporate Rules have been established and approved by IMY, and the recipient of the Personal Data in the third country is subject to them; or

4. The data subject has given their consent to the transfer. This presupposes that the data subject has been informed of the risks of the transfer.

5.2 Brilliant Future has undertaken through data processing agreements not to transfer Personal Data processed on behalf of the customer to third countries. Thus, regardless of whether any of the above conditions apply, Brilliant Future may not transfer Personal Data processed on behalf of Brilliant Future's customers to third countries.

5.3 It should be noted that in some circumstances in may also be necessary to carry out a so-called transfer impact assessment ("**TIA**") prior to transferring data to a third country, despite one of the conditions under section 5.1 is met. Prior to any such transfer being initiated the conditions for the transfer, including the assessment of whether a TIA is necessary, shall be assessed and determined by Brilliant Future's management.

## 6. Data processing agreements, risk and vulnerability assessments and impact assessments

6.1 When Personal Data is disclosed to a third party that Processes the Personal Data on behalf of Brilliant Futures in Brilliant Futures' role as Data Controller, a so-called Data Processor, the handling shall be regulated by a so-called Data processing agreement. Data processing agreements should only be concluded by authorised representatives.

6.2 If the Processor will Process the Personal Data outside the EU/EEA, a Processor Agreement must be supplemented with one of the safeguards in section 5, such as the European Commission's model clauses, thereby ensuring that there is an adequate level of protection in accordance with the Data Protection Rules in the recipient country.

6.3 If the third party engages any other third party (a so-called sub-processor) for the Processing of Personal Data, such as a subcontractor of one of Brilliant Future's suppliers, the same obligations as set out in section 6.1 above shall be imposed on the sub-processor, in particular to ensure sufficient guarantees for the implementation of appropriate technical and organisational security measures. Both Brilliant Future and any Processor should ensure that appropriate technical and organisational measures are put in place to provide adequate protection for Personal Data in different situations.

6.4 In some cases, a risk and vulnerability assessment ("**RVA**") is also necessary. Such an assessment should be carried out when introducing new IT solutions, for

example when using cloud service providers that apply standard terms and conditions. An RVA may also be necessary in certain situations where a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons.

## 7. Processing of Sensitive Personal Data

7.1 Some Personal Data is by its nature particularly sensitive and therefore has a stronger protection under the GDPR. Brilliant Future may in some cases Process Sensitive Personal Data, for example about health. As a starting point, Sensitive Personal Data may not be Processed under the GDPR, but exceptions exist. Before commencing Processing of Sensitive Personal Data, an appropriate support for handling this data should always be identified, such as an explicit consent or a right or obligation that employers must perform such Processing under labour law. If explicit consent is obtained, this should be clearly documented.

## 8. Summary of actions that need to be taken before Processing Personal Data

8.1 The following measures should be taken before any Processing of Personal Data is carried out by a Controller:

a) Determine the purposes and legal basis of the Processing;

b) Enter into a Data Processing Agreement when Personal Data is to be Processed by a third party and Brilliant Future is the Data Controller;

c) Ensure that technical and organisational security measures are in place;

d) If any Processing will take place outside the EU/EEA, appropriate safeguards under the GDPR must be followed; and

e) Ensure that the Data Subject receives all information required by Data Protection Laws and document any consent obtained.

Brilliant

## PART II - PRACTICAL MEASURES FOR PROCESSING PERSONAL DATA

### 9. Introduction

9.1 This section describes practical measures for the Processing of Personal Data within Brilliant Future. Information is provided on the obligations that Brilliant Future act as a Data Controller as well as a Data Processor.

9.2 Further information on the Processing of Personal Data can be found in

- Brilliant - General Information Security Policy.
- Brilliant - Incident Management Process.
- Brilliant – Risk Management Process.
- Brilliant CX-EX-Insight – Architecture Compliance and Security White paper.
- Brilliant CX-Navigator - Architecture Compliance and Security White paper.
- PUB Navigator 251118 ENG
- PUB Insight 251118 ENG

All documents and processes can be found in Brilliant Future's internal Information Security Management System (ISMS) at:

https://brilliantfuture.sharepoint.com/sites/ISMS

### 10. Procedures for data erasure

10.1 Personal data may only be retained for as long as necessary for the relevant purposes of the Processing. This means that data that is no longer necessary to keep must be deleted. Many deletion periods are required by law, for example

- Retention in accordance with the provisions of the Bookkeping Act (1999:1078) should not exceed the legal requirement of seven (7) years.
- Data on job applicants called for an interview should be deleted after two (2) years after the appointment of the position to fulfil the requirements of the Discrimination Act (2008:567).

10.2 Further information on deletion periods for different types of Processing operations can be found in

- Brilliant CX-EX-Insight – Architecture Compliance and Security White paper.
- Brilliant CX-Navigator - Architecture Compliance and Security White paper.

10.3 Where Brilliant Future is acting as Processor, the Personal Data shall, at the choice of the Controller, be erased or returned to the Controller upon termination of the provision of the Service.

## 11. Procedures for the Data Subject's right of access to information

11.1 The Data Subject shall have the right to obtain information about the Personal Data that are Processed about the Data Subject.

11.2 As a starting point, a request for access should be processed within one (1) month. The identity of the Data Subject and the data to which the Data Subject wants access (not everything needs to be disclosed if the Data Subject does not request it) should be verified. Subsequently, it should be analysed whether any exception is applicable where there is no requirement/permission to disclose the Data Subject's Personal Data. Personal Data should then be disclosed, or an explanation should be given as to why Personal Data is not disclosed.

11.3 When acting as a Processor, Brilliant Future shall assist the Controller with requests from the Data Subject to exercise the right to access information about the Personal Data Processed about the Data Subject.

## 12. Procedures for the erasure and rectification of Personal Data

12.1 A Data Subject has the right to have their Personal Data rectified. The Data Subject's instructions should be followed and it should be ensured that Personal Data are rectified immediately when the Data Subject has requested the rectification of their Personal Data.

12.2 In addition, the Data Subject has the right to be erased in certain cases. The Data Subject's Personal Data should be erased if:

- the data are no longer needed for the purposes for which they were collected;
- The Processing is based on the individual's consent and the individual withdraws consent;
- The Processing is for direct marketing purposes and the individual objects to the Processing of the Personal Data; or
- the individual objects to the Processing of Personal Data after a balancing of interests and there are no legitimate grounds which override the interests of the individual.

12.3 Erasure should take place without undue delay. Where Personal Data are erased at the request of the Data Subject, information about the erasure should be provided to those to whom the Personal Data have been disclosed so that they

can also erase the Personal Data. However, this does not apply if it proves impossible or involves a disproportionate effort.

12.4 When acting as a Processor, Brilliant Future shall assist the Controller with requests from the Data Subject to exercise the right to erasure or rectification of Personal Data.

## 13. Procedures for the transfer of Personal Data (data portability)

13.1 Data portability means the right of a Data Subject to move Personal Data from one Controller to another. This situation is mainly aimed at situations where Data Subjects switch digital services, for example in the case of social media. However, as drafted, the rules are relevant in other contexts as well. Personal Data covered by data portability are Personal Data relating to the Data Subject and provided by the Data Subject himself/herself.

13.2 Personal data should be transmitted in a structured, commonly used, machine-readable format.

13.3 Deadline for transfer:

- Without undue delay and no later than one month after receiving the request, the Data Subject should be informed of the action taken. This period may be extended for up to two months in the case of a complex request, provided that the Data Subject has been informed of the reasons for the delay within one month of the initial request.

13.4 A fee may not be charged for providing the Personal Data unless it can be shown that the request is manifestly unfounded or excessive.

13.5 When acting as a Processor, Brilliant Future shall assist the Controller with requests from the Data Subject to exercise the right to data portability.

## 14. Procedures in case of a Personal Data Breach

14.1 If a Personal Data Breach occurs (e.g. data is destroyed or falls into the wrong hands) and this may pose a high risk to Data Subjects affected, there are requirements to take certain measures, including informing IMY and the affected individuals.

14.2 Message to IMY.

- In the case of a Personal Data Breach, the Controller shall notify the Personal Data Breach to IMY without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the Personal Data Breach is unlikely to result in a risk to the rights and

freedoms of natural persons. If the notification is not made within 72 hours, it shall be accompanied by a justification of the delay.

- Where a Processor suffers a Personal Data Breach, the Processor shall notify the Controller without undue delay after becoming aware of the breach.

14.2.1 The notice referred to in point 14.2 shall at least

- describe the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects affected and the categories and approximate number of Personal Data records affected;
- communicate the name and contact details of the Data Protection Officer or other contact points where more information can be obtained;
- describe the likely consequences of the Personal Data Breach; and
- describe the measures taken or proposed by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its potential adverse effects.

14.2.2 If and to the extent that it is not possible to provide the information at the same time, the information may be provided in instalments without undue further delay.

14.2.3 All Personal Data Breaches should be documented, including the circumstances of the Personal Data Breach, its effects and the corrective actions taken. The documentation should enable IMY to verify compliance with Article 33 of the GDPR.

14.3 Information to the Data Subject:

- If the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller should inform the Data Subject of the Personal Data Breach without undue delay.
- The information to the Data Subject should include a clear and unambiguous description of the nature of the Personal Data Breach and at least the information and measures referred to in Section 14.2.1.

14.3.1 Information to the Data Subject in accordance with Section 13.3 is not required if any of the following conditions are met

- Appropriate technical and organisational security measures have been implemented and applied to the Personal Data affected by the Personal Data Breach, in particular those designed to render the data unreadable

to any person not authorised to access the Personal Data, such as encryption.

- Additional measures have been taken to ensure that the high risk to the rights and freedoms of Data Subjects referred to in 14.3 is no longer likely to materialise.
- This would involve a disproportionate effort. In that case, the public shall instead be informed or a similar measure shall be taken whereby Data Subjects are informed in an equally effective manner.

14.4 Notifying the controller

14.4.1 When acting as a Processor, Brilliant Future shall assist the Controller in notifying IMY of the Personal Data Breach and informing Data Subjects of the Personal Data Breach.

14.4.2 The SLA and incident response for Personal Data Breaches is within 1 hour and such notification shall be provided to Brilliant Future's contact person(s) within the controller's organization unless a separate contact point has been agreed with the specific controller for this specific purpose. The incident team is responsible for notifying the data controller, all involved data processors and, if applicable, IMY. Personal data breaches must be reported by the controller to IMY within 72 hours.

The Incident Management Process further describes the routines for notifying IMY, data controller and sub-processors.

## 15. Procedures for access and transfer of Personal Data

15.1 Access and transmission of Personal Data, for example over open networks, requires in some cases strong encryption standards and sometimes also two-step authentication. Special protection applies, inter alia, to Sensitive Personal Data, data relating to criminal offences and data subject to confidentiality or special legal requirements. Information should be categorised according to its sensitivity and protection value, to ensure that adequate security measures are taken.

15.2 Employees who have access to Sensitive Personal Data should not print, save, copy or take screenshots of Sensitive Personal Data.

15.3 Sensitive Personal Data and other data requiring protection should also not be transferred over an open network, such as the internet or via a web-based e-mail. An example of when this should be observed is when Personal Data is transferred between employees.

## 16. Marketing and other communications

16.1 If a Data Subject has objected to direct marketing by email or other communication, the Data Subject's request should be implemented without undue delay. The same applies if the Data Subject wishes to refrain from sharing their Personal Data with third parties.

16.2 If the Data Subject has objected to direct marketing by email, other communications or to sharing information with third parties, it should be ensured that:

- the Data Subject's e-mail address and/or other contact details of the Data Subject are no longer subject to automatic e-mailing and/or
- a request is sent to all third parties concerned, instructing them to delete the information and Personal Data of the Data Subject and to ensure that all system settings enabling automatic mailings are immediately removed from the Data Subject.