



Internal Privacy Notice

1. Policy Statement

Britvic PLC and its group companies ("we" or "us") is, in relation to certain types of personal data, a "data controller" and we have issued this Privacy Notice (this "notice") to describe how we hold and use personal data about you. To view the list of Britvic companies in the EEA that are considered 'data controller', please go to Appendix 2.

We respect the privacy rights of individuals and are committed to handling personal data responsibly and in accordance with the UK General Data Protection Regulation (UK GDPR) and all other applicable law which says that the personal data we hold about you must be:

- used lawfully, fairly and in a transparent way;
- collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- relevant to the purposes we have told you about and limited only to those purposes;
- accurate and kept up to date;
- kept only as long as necessary for the purposes we have told you about; and
- kept securely.

This notice sets out the personal data that we collect and process about you, the purposes of the processing and the rights that you have in connection with it.

2. Policy Owner

Kevin Blake, Director of Reward & HR Services

3. Who does it apply to?

This notice describes how we handle personal data that we hold about our employees, workers (temporary and permanent), contractors, consultants, secondees, interns and other third parties engaged to carry out work for us and who have access to our premises or our internal systems.

4. What is covered in this notice?

In this notice we explain:

- what the key terms "personal data", "special category personal data" and "processing" mean;
- why we process your personal data;
- where the data comes from;
- how long we keep your personal data;
- the legal grounds which allow us to process your personal data;
- our approach to automated decision making
- how we ensure your personal data is secure;
- who gets to see your personal data;
- how to access your personal data and other rights you have; and
- who to contact if you have any questions or want to make a complaint.

5. Key terms

What is "personal data"?

"Personal data" is any information about you from which you can be identified. It includes not only facts about you, but also intentions and opinions about you. It does not include data where your identity has been removed (i.e. anonymous data).

What is "special category personal data"?

"Special category personal data" is a sensitive type of personal data which requires a higher level of protection, namely:

- information about your race or ethnicity, religious beliefs, sexual orientation and political opinions;
- trade union membership;
- information about your health, including any medical condition, health and sickness records;
- genetic information and biometric data; and
- information about criminal convictions and offences.

What is "processing"?

"Processing" means doing anything with the data. For example, it includes collecting it, holding it, disclosing it and deleting it.

6. Why do we process your personal data?

There are various reasons why we need to process your personal data for the purpose of our business, including management, administrative, employment and legal purposes. A non-exhaustive list of the purposes for which we will process your personal data is set out in Appendix 1 to this notice.

7. Where does the data come from?

When you start working with us, the initial personal data about you that we process is likely to come from you: for example, contact details, bank details and information on your immigration status and whether you can lawfully work. We may also, where necessary, require references and information to carry out background checks. In the course of your engagement with us, you may be required to provide us with information for other purposes such as discretionary or statutory sick pay and family rights (e.g. maternity and paternity leave and pay). If you do not provide information (or exercise your right to erasure) that you are required by law or contract to give us, you may lose benefits or we may decide not to employ you or to end your contract. If you have concerns about this in a particular context, you should contact HR Services.

In the course of your work, we may receive personal data relating to you from others. Internally, personal data may be derived from your managers and other colleagues or our IT systems; externally, it may be derived from our suppliers, customers, or those to whom you communicate by email or other systems.

8. How long do we keep your personal data?

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different types of personal data set out in our Document Retention Policy.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Once you no longer work with us, we will retain and securely destroy your personal information in accordance with our Document Retention Policy.

Our Document Retention Policy is available to you on MyCompass.

9. The lawful basis for processing personal data

What is the lawful basis for processing “personal data”?

Our lawful basis for collecting and using your personal data will depend on the personal information concerned and the specific context in which we collect it, but we will rely on one or more permitted lawful grounds as laid down by the UK GDPR, as summarised and explained in the table on the next page:

Lawful basis for processing	Defined term for the purpose of this notice	Explanation
You have given specific consent to us processing your data	"Consent"	In general, the processing of your personal data in connection with your employment/service contract does not require your consent. However, there may be occasions where we request your specific consent to process your personal data
The processing is necessary for the performance of a contract with you or to take steps at your request to enter a contract	"Contract"	This covers carrying out our contractual duties and exercising our contractual rights
The processing is necessary to comply with our legal obligations	"Legal obligation"	Ensuring we perform our legal and regulatory obligations. For example, providing a safe place of work, providing data to HMRC, Revenue (or any other local or national tax authorities as applicable), and avoiding unlawful discrimination

<p>The processing necessary for our (or a third party's) legitimate interests</p>	<p>"Legitimate interests"</p>	<p>We or a third party have legitimate interests in carrying on, managing and administering our respective businesses effectively and properly and in connection with those interests, processing your data. Your data will not be processed on this basis if our (or a third party's) interests are overridden by your own interests, rights and freedoms</p>
---	--------------------------------------	--

If you have questions about or need further information concerning the lawful basis on which we process your personal information, please contact Britvic's Data Protection Officer.

What is the lawful basis for processing “special category personal data”?

As explained above, special category personal data requires a higher level of protection than normal personal data. In addition to the grounds for processing normal personal data already mentioned, we also need to have further justification for collecting, storing and using this type of personal data. Those further justifications include:

- with your explicit consent;
- where we need to carry out our legal obligations or exercise rights in connection with employment;
- where we need a medical diagnosis, and / or assessment of your working capacity; or
- where it is necessary for reasons of substantial public interest, such as for equality and diversity monitoring.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public (e.g. if you tell colleagues that you are ill).

We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing special category personal data.

Here are some examples of the ways we may use your special category personal data:

- we may use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws;
- we may use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits;
- we may use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting; and
- we may use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

Further information on the personal data that we process

Further information on the types of personal data we may process in relation to you, the purpose for which that data may be processed and the lawful grounds for such processing is set out in Appendix 1 to this notice.

10. Data security

We have put in place measures to protect the security of your data. Details of these measures are set out in our IT Policy which is available on MyCompass.

Third parties will only process your personal data on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures are set out in our IT Policy which is available on MyCompass.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

11. Who gets to see your data?

Internal use

Where necessary and as set out in this privacy notice, your personal data will be shared with your managers, HR and administrators for employment, administrative and management purposes as mentioned in this document.

We will where necessary and as set out in this privacy notice also share your personal data with other members of our Britvic group of companies around the world in order to administer human resources, staff member compensation and benefits at an international level on the HR System, as well as for other legitimate business purposes such as IT services/security, tax and accounting, and general business management.

External use (sharing outside of the Britvic group)

In addition, we will share your personal data with certain organisations outside the Britvic group who provide services to us. For example, some personal data will be disclosed to our employee pension and benefit plans service providers and organisations who provide us with payroll support services, relocation, tax and travel management services, as well as the providers of our IT services and systems. All of our service providers are required to take appropriate security measures to protect your personal data in line with our policies.

We will only share your personal data with organisations outside the Britvic group if that disclosure is consistent with a ground for processing on which we rely and doing so is lawful and fair to you. Generally, we will do so where it is necessary for our legitimate interests as an organisation or the interests of a third party (but we will not do this if these interests are over-riden by your interests and rights in particular to privacy).

Sometimes we may disclose personal information to organisations outside the Britvic group on other lawful grounds, such as:

- to comply with our legal obligations, including where necessary to abide by law, regulation or contract, or to respond to a court order, administrative or judicial process, including, but not limited to, a subpoena, government audit or search warrant;
- in response to lawful requests by public authorities (including for national security or law enforcement purposes);
- as necessary to establish, exercise or defend against potential, threatened or actual litigation;
- where necessary to protect the vital interests of you or another person;
- in connection with the sale, assignment or other transfer of all or part of our business; and/or
- with your consent.

12. Transfers of personal data outside the European Economic Area (EEA)

We may transfer some of the personal data we collect about you to the following countries and territories outside the EEA: The United States of America, Canada, India, Singapore, Hong Kong, South Africa, Australia and Malaysia.

There is an adequacy decision by the European Commission in respect of Canada (commercial organisations), meaning that commercial organisations within Canada to which we transfer your data are deemed to provide an adequate level of protection for your personal data.

There is not an adequacy decision by the European Commission in respect of the other countries and territories listed above, meaning that those countries are not deemed to provide an adequate level of protection for your personal data.

However, to ensure that your personal data does receive an adequate level of protection, we have put in place standard contractual clauses, to ensure that your personal data is treated in a way that is consistent with and which respects UK and EU laws on data protection. If you require further information about these protective measures, you can request it from Britvic's Data Protection Officer.

13. Access to your personal data and your other data rights

We try to be as open as we reasonably can about personal data that we process. If you would like specific information, just ask our HR Services or Britvic's Data Protection Officer.

Your data rights

You have the right:

- to ask us for copies of your personal data (**right to access**);
- to ask for inaccurate personal data to be corrected or made complete (**right to rectification**);
- to ask for your personal data to be deleted (**right to erasure**);

- to ask us to limit the way we use your personal data if you are concerned about its accuracy or how it is used (**right to restriction of processing**);
- to object to us using your personal data where we are using it for ours or a third party's legitimate interests, or where we are using it for direct marketing (**right to object**);
- to ask us to transfer your personal data to another data controller (**right to data portability**);
- not to be subject to a decision based solely on automated processing, including profiling;
- to withdraw consent at any time (to the extent that we rely on it as a basis for processing); and
- to complain to a supervisory authority. In the UK, you can complain to the Information Commissioner's Office. To make a complaint, visit <https://ico.org.uk/concerns/>. In the event of a concern about how your personal data are being handled, you are asked first to raise that concern with us by HR Services or Britvic's Data Protection Officer.

Please note that many of these rights are not absolute – the extent to which they apply may vary depending on the particular circumstances and any applicable exemptions. It means that in some situations we may not comply with your request.

How to exercise your data rights

You may exercise your data rights (as summarised above) as follows:

- if you wish to access, correct, update or request deletion of your personal information, you can do so at any time by contacting HR Services;
- in addition you can object to processing of your personal information, ask us to restrict processing of your personal information or request portability of your personal information by contacting HR Services; and

- if we have collected and processed your personal information with your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent. To withdraw your consent, please contact HR Services.

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws, as outlined in our Data Subject Rights Handling Guidance which is available on MyCompass.

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current, so please let us know if your personal information changes during your working relationship with us.

14. Questions or Complaints

If you have any questions related to this notice, you can either raise this with your line manager or HR Services via [askHR](#) (please select GDPR General category).

If you have complaints relating to our processing of your personal data, you should raise these with our Data Protection Officer at DataPrivacy@britvic.com. You also have the right to raise a complaint with the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues, or any other local or national body responsible for regulating data protection.

15. Status and updates to this notice

This notice does not form part of your contract of employment or other contract to provide services and it does not create contractual rights or obligations.

This notice may be updated from time-to-time to reflect any necessary changes in our privacy practices.

In such cases, we will inform you via MyCompass or another appropriate communication method. We encourage you to check back periodically in order to ensure you are aware of the most recent version of this notice.

16. What other documents do I need to know about?

- [Data Privacy and Personal Information Policy](#)
- [Data Subject Rights Guidance](#)
- [Document Retention Policy](#)
- [IT Policy](#)
- [Major Business Incident Management Policy](#)

Appendix 1 - further information on the personal data that we process and our purposes

The examples in the below table cannot, of course, be exhaustive. For example, although the table does not mention data relating to criminal offences, if we were to find out that someone working for us was suspected of committing a criminal offence, we will process that information if relevant for our purposes. If necessary we will also require criminal background checks for certain roles.

Purpose	Examples of personal data that may be processed	Lawful basis for processing
Recruitment, background checks, onboarding and emergency contact information	Name, contact details (address, email, telephone number), date of birth, emergency contact information / next of kin, NI number, education and training, CV, references, work permit, sickness and health information, ID such as passport and driving licence, racial / ethnic origin and Trade Union membership	Legitimate interests Legal obligation
Entering into the contract and terminating the contract	Name, contact details, date of birth, NI number, providing references, employment status, work permit, sickness and health information, passport / driving licence, criminal background and contractual terms	Legitimate interests Legal obligation Contract

Training and performance including succession and talent records	Name, contact information, training and performance management records (myPerformance), personal opinion, employment status, contractual terms including Band	Legitimate interests Contract
Compensation and benefits, including pension	Name, contact information, date of birth, NI number, bank account information, employment status, sickness records, salary and bonus information, pension and benefits schemes	Legitimate interests Legal obligation Contract
Processing payroll, administration and record-keeping	Name, contact information, employment status, bank account information, sickness, salary, bonus and pension information, benefit schemes and leave information (e.g. parental leave, annual leave)	Legitimate interests Legal obligation Contract
Health information	Name, contact information, health information including occupational health reports and return to work plans, employment status, sickness absence and reasonable adjustments	Legitimate interests Legal obligation

Disciplinary and grievance (internal complaint) processes	Name, contact and employment information, disciplinary and performance management records, complaint records and relevant investigations (which may include CCTV monitoring data)	Legitimate interests Legal obligation Contract
Equal opportunities, diversity monitoring	Name, racial / ethnic origin, age range, gender, sexual orientation, religion, disability, gender identity	Legitimate interests
Disputes and legal proceedings	Name, contact information, employment status, dispute and litigation records	Legitimate interests Legal obligation
Employee feedback (including engagement surveys and exit interviews)	Name, contact and employment information, employment status, date of birth, personal opinion and information from you about your experiences of working for us	Legitimate interests
People analytics – to measure key HR metrics	Name/identifier, gender, employment status, contractual terms including Band	Legitimate interests
CCTV monitoring, access and system usage and security	Site CCTV for security purposes and in the event of an incident, records of the use of electronic access systems and records of your use of our systems including computers, internal-facing websites and digital platforms, phones and other devices and passwords	CCTV monitoring, access and system usage and security

IT information	Information required to provide access to company IT systems and networks, such as name, contact information, location, IP addresses, log files and login information	Legitimate interests
Accident reporting (RIDDOR) and other Health and Safety records	Name, contact information, health and safety records, date of birth, any photo's or video evidence and your employment status	Legitimate interests Legal obligation
Managing payment of business expenses	Name, contact information, employee number or unique identifier, band, job title, bank details and information about your expenses claims	Legitimate interests

Appendix 2 – List of Britvic entities in the EEA that are considered 'data controllers'

Registered Office	Entity Name
GB	Britvic Plc
GB	Britvic Northern Ireland Pensions Limited
GB	Britvic Soft Drinks Limited
GB	Britvic EMEA Limited
Ireland	Britvic Ireland Limited
Ireland	Britvic Northern Ireland Limited
Ireland	Counterpoint Wholesale (Ireland) Limited

GB	Counterpoint Wholesale (NI) Limited
Ireland	Aquaporte Limited
France	Teisseire France SAS
France	Fruite SAS
France	Bricfruit SAS
France	Unisource SAS