BAUER DATA PROTECTION POLICY

Bauer Media - Data Protection Policy

Introduction

Bauer Media needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy sets out how this personal data must be collected, handled and stored to meet Bauer's data protection standards and to comply with the General Data Protection Regulation ('GDPR') and applies to all employees, contractors and freelancers working on behalf of Bauer.

Why this policy exists

This policy exists to ensure Bauer:

- complies with data protection law and follows good practice;
- protect the rights of employees, customers and clients;
- is open about how we store and process individual's data;
- protect ourselves from the risks of a data breach.

Data Protection Law

GDPR describes how organisations must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically or on paper.

GDPR is underpinned by eight important principles:

The right to be informed: organisations are obliged to provide "fair processing information", typically though a privacy notice and to be transparent over how they use personal data;

The right of access: organisations are obliged to provide individuals with confirmation that their data is being process, access to the data held about them and any other supplementary information;

The right to rectification: organisations are obliged to rectify any inaccurate or incomplete personal data, and where appropriate inform any third parties to whom the data has been disclosed;

The right to erasure: organisations are obliged to provide individuals with "the right to be forgotten" such that all personal data is either deleted or removed;

The right to restrict: organisations are obliged to provide individuals the ability to "block" or suppress processing of personal data held in certain circumstances;

The right to portability: organisations are obliged to allow individuals to obtain and reuse their personal data for their own purposes;

The right to object: organisations are obliged to inform individuals of this right and provide the ability to object to the processing of their data on the grounds, in relation to their particular situation;

The right not to be subject to automated decision-making: organisation are obliged to provide safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

Important Definitions

What is Personal Data?

"Personal" data is information that relates to a living individual who can be identified from that information or from that information and other information in possession of the data controller. For example, name, address, telephone number or email address. Personal data includes any expression of opinion about the individual and any indication of the intentions of the data controller in respect of that individual.

What is 'Sensitive' Personal Data?

This is distinct from non-sensitive or "ordinary" personal data and is specifically dealt with in GDPR. It includes details of racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions.

The Data Controller

Any person or entity who either alone or in common with other persons determines the purposes for which and the manner which any personal data can be processed. Bauer Media are a "Data Controller" of the personal details that staff collect from the public.

Data Subjects

Data Subjects are any living individual who is the subject of personal data.

Role of the Data Protection Officer

Bauer's Data Protection Officer is Susan Voss.

The Data Protection Officer is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies.
- Arranging and monitoring data protection training.
- Handling data protection questions from employees and anyone less covered by this policy.
- Dealing with subject access request.
- Checking and approving any contracts or agreements with third parties that may handle Bauer personal data.

All breaches or potential breaches should be reported to the Data Protection Officer immediately.

Handling of personal/sensitive information

Bauer Media will, through appropriate management and the use of strict criteria and controls: -

- Ensure the fair collection and use of personal data;
- Meet its legal obligations clearly to notify to data subjects the purpose for which their personal data is to be used at the time it is collected from them;

- Collect and process appropriate personal data and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of personal data used;
- Apply strict checks to determine the length of time personal data is held;
- Take appropriate technical and organisational security measures to safeguard the confidentiality and prevent unauthorised processing (including disclosure) of personal data;
- Ensure that personal data is not transferred outside the EU without suitable safeguards.

In addition, Bauer Media will ensure that:

- There is someone with specific responsibility for data protection in the organisation to act as a point of contact for queries and to ensure the day-to-day implementation of this Policy;
- Everyone managing and handling personal data understands that they are contractually responsible for following good data protection practice and being aware of and following this Policy;
- Everyone managing and handling personal data is appropriately trained to do so;
- Everyone managing and handling personal data is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal data from the public are promptly and courteously dealt with;
- Methods of handling personal data are regularly assessed and evaluated in the light of ongoing regulation.

Subject Access Requests

Bauer Media respects the rights of individuals ('data subjects') under the GDPR.

These include:

- The right to be informed that processing is being undertaken;
- The right of access to one's personal information within 30 days; (a "Subject Access Request");
- The right to prevent processing in certain circumstances;
- The right to correct, rectify, block or erase information regarded as wrong information.
- The right to be forgotten.

Any Subject Access Request should be passed to the Data Protection Officer.

In certain circumstances personal data can be disclosed to law enforcement agencies without consent of the data subject.

Under these circumstances, Bauer will disclose requested data. However, the Data Protection Officer will ensure that the request is legitimate.

General Staff Guidelines

All employees must ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Annual training must be completed by all employees.
- All data is kept secure, by taking sensible precautions.
- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment behind locked doors and disposed of securely, e.g. by shredding;

- Personal data held on computers and computer systems is protected by the use of secure passwords, which (where possible) have forced changes periodically and must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- All such personal data should be stored on the Bauer network drives and not locally.
- Individual passwords should be such that they are not easily compromised and never shared between employees.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- Data being transferred electronically must be password protected and if possible not sent by email as this form of communication is not secured.
- All servers and computers containing data should be protected by approved security software and a firewall.
- Screens of computers should always be locked when left unattended.
- "Sensitive" personal data should always be considered separately and the Data Protection Officer notified. The same applies to any other personal data that could be considered private or confidential or which could cause damage or distress if released.
- Data should be regularly reviewed and update if it is found to be out of date. If no longer required, it should be securely deleted.
- The Data Protection Officer has day-to-day responsibility for the security of personal data and from time-to-time may require appropriate staff to attend internal training sessions.
- Any new data process must not be undertaken until a Data Impact Assessment has been completed.

Working with Third Parties

All third parties must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of Bauer Media, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under GDPR.
- Data sharing is only carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures and may only be undertaken with reputable third parties who offer compliance with GDPR.
- Their compliance with GDPR should be checked and verified.

Rules Regarding Permission to Contact

- Consent requires a positive opt-in, we cannot use pre-ticked boxes, opt out or any other method of consent by default.
- Consent means offering individuals genuine choice and control.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.
- Be specific and granular. Vague or blanket consent is not enough. You will require separate permission for email, phone and post.
- Be clear and concise.
- Name any third parties who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent - who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Do not make consent a precondition of a service.
- Ensure that approved wording is used at all times.

Providing information

Bauer aims to ensure that individuals are aware that their data is being processed and they understand:

- How the data is being used
- How to exercise their rights

This information is set out in our privacy policy link here

Contacts

If you have any queries please contact Susan Voss who acts as the Data Protection Officer for Bauer Media or a member of the legal team.

BAUER DATA PROTECTION POLICY

Document Control

Document	Data Protection Policy
Document Owner	Bauer Data Protection Officer

Version History

Version	Date of Revision	Summary of Changes
Version 1	01/05/18	GDPR required changes in legislation
Version 2	16/10/20	Changes to Privacy Policy, updated document links

Approvers

This document requires the following approvals

Role	Name
Data Protection Officer	Susan Voss