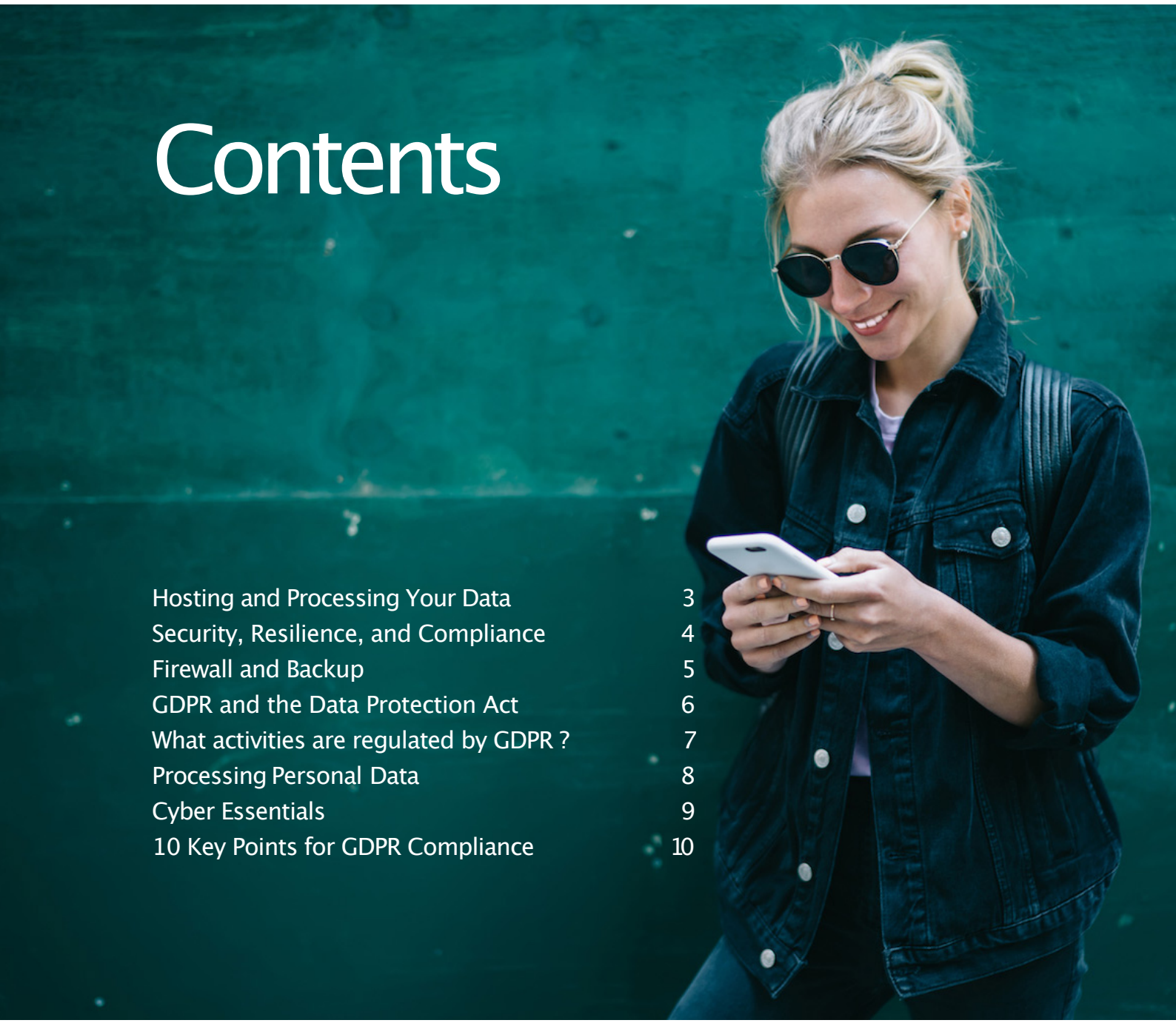
WHITE BEAR

Hosting and Processing Your Data

Privacy, Security, Compliance, Data Protection & Information Governance



Contents

Hosting and Processing Your Data

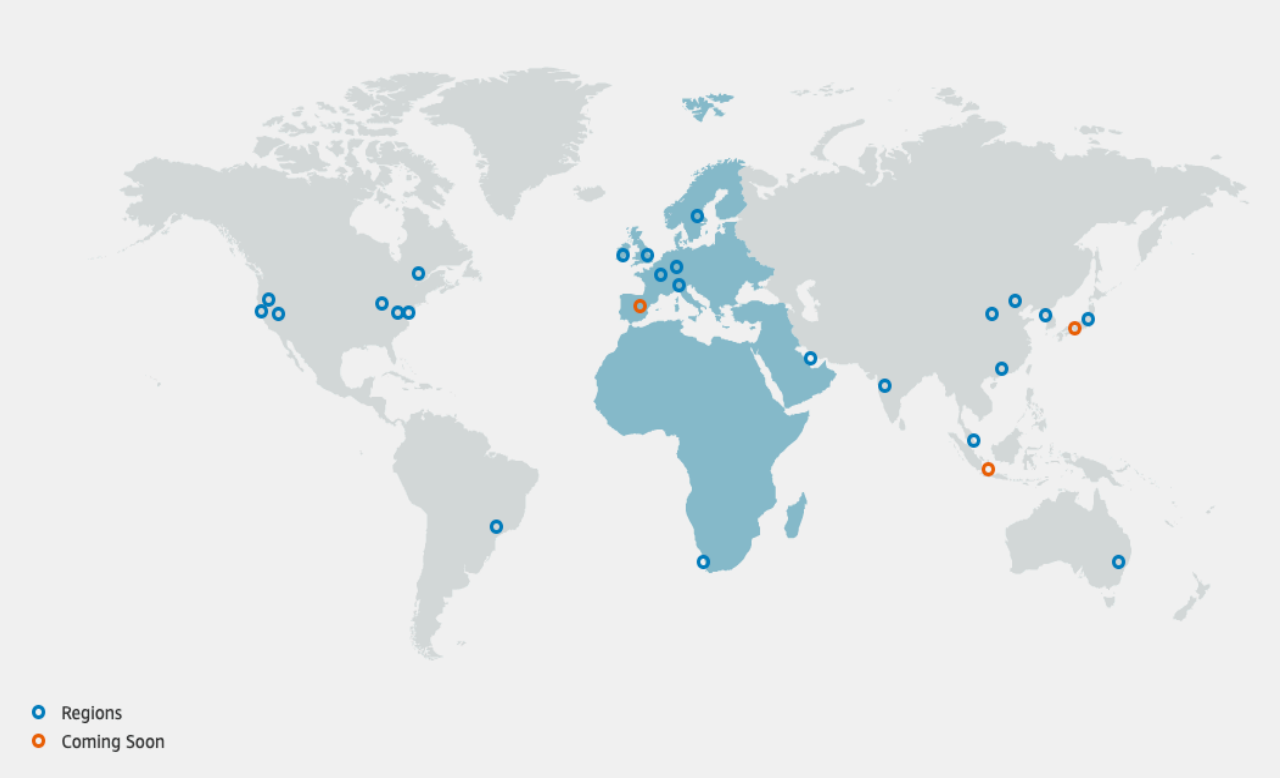
White Bear Digital use cloud hosting solutions provided and supported by Amazon Web Services (AWS) and manage them for our clients. AWS provides businesses, non-profits, and governmental organisations with a flexible, highly scalable, and a low-cost way to deliver their websites and web applications.

Amazon AWS is one of the world's largest and longest-established cloud computing platforms, and is used by companies of all sizes, from startups to household names. AWS is a playing field leveller, enabling any size business to leverage high-end technologies and infrastructure. Amazon AWS has been delivering global infrastructure at a large scale since 2006.

Amazon AWS infrastructure is hosted across the globe, although at White Bear all of the data we process and our hosting is located in the EU or UK.

For any business that collects data, website traffic can fluctuate a lot. From quiet times in the middle of the night, to campaign driven, social media sharing traffic spikes, White Bear provide a very flexible computing infrastructure that can grow and shrink to meet your needs.

Global Infrastructure – EU/UK Focus



Security, Resilience, and Compliance

AWS offers our clients peace of mind when it comes to security and compliance for the storage and processing of their data.
ISO 9001, ISO 27001, ISO 27017, ISO 27018, PCI DSS Level 1, HIPAA, and G–Cloud are among the well–recognised certifications that Amazon AWS holds.

• The AWS infrastructure puts strong safeguards in place to help protect customer privacy. Data centres are physically secured, and any user access to data is controlled and minimised.

• White Bear retain complete control and ownership over the region in which your data is physically located, making it easy to meet regional compliance and data residency requirements. All data processed by White Bear is stored in highly secure EU or UK based AWS data centres.

• Multiple geographic regions and Availability Zones allow us to remain resilient in the face of most failure modes, including natural disasters or system failures.

• Ability to configure built–in firewall rules from totally public to completely private or somewhere in between to control access to instances.

• AWS delivers highly scalable managed services for database, caching, data–warehousing, transcoding, storage, backup, infrastructure management & application management.

• The data we process for clients at White Bear is stored in secure databases, with multiple synchronised copies across multiple EU data centre locations.

Firewall and Backup

The biggest contributing factor to website hacks today comes from insecure code. With enough time, and new techniques, attackers find ways to exploit weaknesses in code.

A Web Application Firewall alongside other protections helps stop these vulnerabilities from being exploited. Prevention and protection is the key.

White Bear provide as standard both a Network Firewall and a Web Application Firewall by Pressidium that protect your website and data. Data is encrypted in transit and transmitted to our secure Amazon AWS servers to be processed.

All websites and data are backed up daily, to a secure remote location. It's the most reliable way to make sure everything stays safe in case disaster strikes.

- Automated off-site backups
- Infrastructure scales on demand
- Fault tolerant and high-availability
- Website Application Firewall (WAF)
- Distributed Denial of Service mitigation
- Malware monitoring and removal
- Expert Support
- Backups of website and processed data

We offer our clients peace of mind and professional support

Defence in Depth: A layered approach to proactive and reactive website security

Protection: Both Network-Based and Website Application Firewalls

Detection: Continuous website security monitoring to quickly identify potential threats

PRESSIDIUM

powered by aws

GDPR and the Data Protection Act

The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. As a data processor for your information, White Bear hold the necessary experience and certification to process personal data effectively and support our clients and individuals who are data controllers.

GDPR and the Data Protection Act 2018 require every organisation that processes personal information to register with the Information Commissioner's Office (ICO), unless they are exempt. Failure to do so is a criminal offence. White Bear is registered with the ICO, our Registration Number is ZA722494

What activities are regulated by GDPR and the Data Protection Act ?

The Data Protection Act 2018 regulates the "processing" of personal data

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –

(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data.

The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles lie at the heart of our approach to processing personal data.

Processing Personal Data

The GDPR applies to the processing of personal data that is:

- wholly or partly by automated means; or
- the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.

Personal data only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.

Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.

If personal data can be truly anonymised then the anonymised data is not subject to the GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.

Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR.

Information about companies or public authorities is not personal data.
However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data

What are the lawful bases for data processing ?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever we process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Cyber Essentials

In addition to the compliance protections at Amazon AWS and Pressidium, White Bear is also Cyber Essentials certified, our certificate number is 0706583859955686.

Cyber Essentials is a UK government scheme supported by the NCSC (National Cyber Security Centre) that sets out five security controls to protect organisations against around 80% of common cyber attacks.

From 1 October 2014, UK Government has required all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme.

The Cyber Essentials scheme is a cyber security standard, which organisations can be assessed and certified against. It identifies the security controls that an organisation must have in place within their IT systems in order to have confidence that they are addressing cyber security effectively and mitigating the risk from Internet-based threats.

The scheme focuses on the following five essential mitigation strategies:

- Boundary Firewalls and Internet Gateways
- Secure Configuration
- Access Control
- Malware Protection
- Patch Management

10 Key Points for GDPR Compliance for White Bear Digital and you

1. Lawful, fair and transparent processing

The organisations that process personal data are asked to process the personal data in a lawful, fair and transparent manner.

- Lawful means all processing should be based on a legitimate purpose.
- Fair means organisations take responsibility and do not process data for any purpose other than the legitimate purposes.
- Transparent means that organisations must inform data subjects about the processing activities on their personal data.

2. Limitation of purpose, data and storage

Organisations are expected to limit data processing, collect only that data which is necessary, and not keep personal data once the processing purpose is completed. This would effectively bring the following requirements:

- Forbid processing of personal data outside the legitimate purpose for which the personal data was collected
- Mandate that no personal data, other than what is necessary, be requested
- Ask that personal data should be deleted once the legitimate purpose for which it was collected is fulfilled

3. Data subject rights

The data subjects have been assigned the right to ask the organisation what information it has about them, and what the organisation does with this information. In addition, a data subject has the right to ask for correction, object to processing, lodge a complaint, or ask for the deletion or transfer of their personal data.

4. Consent

As and when the organisation has the intent to process personal data beyond the legitimate purpose for which that data was collected, a clear and explicit consent must be asked from the data subject. Once collected, this consent must be documented, and the data subject is allowed to withdraw their consent at any moment.

Also, for the processing of children's data, GDPR requires explicit consent of the parents (or guardian) if the child's age is under 16.

5. Personal data breaches

The organisation must maintain a Personal Data Breach Register and, based on severity, the regulator and data subject should be informed within 72 hours of identifying the breach.

6. Privacy By Design

Organisations should incorporate mechanisms to protect personal data in the design of new systems and processes; that is, privacy and protection aspects should be ensured by default.

7. Data Protection Impact Assessment

To estimate the impact of changes or new actions, a Data Protection Impact Assessment should be conducted when initiating a new project, change, or product. The Data Protection Impact Assessment is a procedure that needs to be carried out when a significant change is introduced in the processing of personal data. This change could be a new process, or a change to an existing process that alters the way personal data is being processed.

8. Data Transfers

The controller of personal data has the accountability to ensure that personal data is protected and GDPR requirements respected, even if processing is being done by a third party. This means controllers have the obligation to ensure the protection and privacy of personal data when that data is being transferred outside the company, to a third party and / or other entity within the same company. When dealing with our clients' data, White Bear Digital is a Data Processor, the client organisation remains the Data Controller.

9. Data Protection Officer

When there is significant processing of personal data in an organisation, the organisation should assign a Data Protection Officer. When assigned, the Data Protection Officer would have the responsibility of advising the company about compliance with EU GDPR requirements. White Bear Digital has chosen to voluntarily appoint a DPO, in excess of the requirements for our business, to help us to maintain data protection mechanisms ad compliance.

10. Awareness and Training

Organisations must create awareness among employees about key GDPR requirements, and conduct regular training to ensure that employees remain aware of their responsibilities with regard to the protection of personal data and identification of personal data breaches as soon as possible. All of our staff are trained on data protection and privacy in excess of the GDPR requirements.

Together we're making a difference

White Bear works in partnership with many leading health institutions, housing organisations, and local authorities. There's so much you can achieve using smarter digital intelligence.

We support our clients to make people's lives better and improve awareness of how our health and care systems can be enhanced.

We're making a difference, and so are you.

Call: 01902 239 077
Email: hello@wearewhitebear.com
Visit: https://wearewhitebear.com/

WHITE BEAR