Bertram Books

The relationship we have with our customers is extremely important to us. We aspire to provide excellent service and operate with utmost integrity at all times. Regardless of regulations that may be in place from time to time (e.g. the General Data Protection Regulation GDPR that comes into force on the 25 May 2018), we treat any Personal Data you share with us as you would want it to be treated; confidentially, securely and only for the purposes it was given for.

Given the importance of GDPR and how far reaching it is, we understand that this has raised questions regarding Personal Data compliance practices across the world and up and down the supply chain. We are no different. We would therefore like to publicise how we meet the regulations contained with GDPR.

Our Commitment To You	Bertrams Position
1. A **Data Protection / Information Security Officer (ISO) has been assigned** to effective govern Data Protection / Information Security practices and continually improve.	We have had an Information Security Office in place for many years. Since April 2017, Chris Good, has been our ISO.
2. All **staff who handle Personal Data have been informed of the upcoming changes to the data protection regulation**, their role and how to report breaches.	• All colleagues have attended face to face Information Security training, and this is mandatory part to a new starters induction programme. • All colleagues must sign up to our IT & Data Policy – providing details of Data Protection regulations and responsibilities. Signoffs are required every two years or whenever a material change is made. • Where a colleague performs a Data Processor role as part of a wider Personal Data Handling Process, they receive targeted training from the corresponding Data Controller (senior leadership members). This is embedded within the new starter induction programme.
3. **Breach reporting processes are in place** between a) us and the Information Commissioners Office (must be completed within 72 hours of the breach occurring), and b) us and the individuals impacted by any Personal Data breaches.	Whilst we strive for zero breaches, mistakes can happen. When they do, our principle is to act quickly and transparently, and learn from what has happened to prevent the same mistake from happening again. A full Information Security / Data Breach reporting procedure is in place, and this is part of the aforementioned IT & Data policy and associated training. If a breach is identified, the employee must first report to their line manager. If the line manager confirms that there is a security/data breach, this must be reported to the Information Security Officer: • If Minor, the line manager leads on establishing a crash team and resolving. The ISO then assesses the actions taken and if any preventative actions are required. • If Major, the ISO leads from start to finish. Assessments are made (using objective criteria) on the need to notify the ICO and/or wider customer communications. We strive to be as transparent as possible, and we lean on the side of wider communication if there is any doubt.

4.	**Personal Data Handling processes have been documented**	Processes are fully documented. The associated Process Owner is responsible for maintaining the process. Reviews are held annually to identify any potential non-compliance or improvement opportunities, or when any material changes to wider processes occur, or if a breach has occurred.
5.	**A Personal Data Inventory has been completed** (what do we hold, why, how was it obtained, how long are we going to retain it for, is it stored securely, is it ever shared with third parties, etc.)	Personal Data inventories have been fully documented for each Personal Data Handling process.
6.	**A Personal Data Inventory has been completed with those third parties that process our / our customer's Personal Data**	For Bertrams front end Business Processing activities, we do not utilise any third parties. For back office functions, robust contracts are in place to ensure suppliers handle Personal Data in the same way we do. Major contracts have already been reviewed and we are continuing to work with all suppliers to ensure obligations are clear and transparent.
7.	For 4, 5 and 6, **weaknesses have been identified and addressed**.	Yes, and we apply a continual service improvement principle, taking into consideration customer needs, regulations and the latest industry capabilities.
8.	**Customer data privacy notices** inform customers that we are capturing their data, what we will use it for, the legal basis for doing so, who it will be disclosed to, whether their data will go outside of the EEA, how long we will retain the data for, their right to complain to the ICO, their right to be deleted and for their data to be ported, and notifying them if we intend to use their data for automated decision making.	Yes. These are available on our website here Update notifications have been circulated via email
9.	**Personal Data is retained and handled in a manner that is compliant to the GDPR compliant Privacy Notices.**	Yes.
10.	**Processes are in place to handle your requests to port across any data we hold about you, to have inaccuracies corrected and to be deleted.**	Manual processes are already in place. We are working on automating this
11.	**Personal Data privacy is embedded within the design of projects and system implementations**, and Data Protection Impact Assessments (DPIAs) are performed before any high risk projects goes live.	'Privacy By Design' has been at the heart of our 'Design For Service' principle for all Projects for many years.