



## Data Protection

PS Financials Ltd complies with the Data Protection Act 1998 and any equivalent binding UK legislation (new Data Protection Bill) and incorporating the General Data Protection Regulation ('GDPR') which will come into force on 25<sup>th</sup> May 2018.

**PS Financials provides an online training and GDPR compliance monitoring service, which can be found by following this link: - <https://www.gdpr.co.uk/?ref=psfinancials>**

PS Financials Ltd will not divulge any of the Customer's confidential information to any person except to its own officers, employees, agents and representatives and then only to who need access to that information to enable PS Financials to fulfil its contractual obligations to the Customer. We confirm that if PS Financials Ltd processes any Service Data on the Customer's behalf when performing its obligations, then the Customer shall be the data controller and PSF shall be a data processor, and that:

1. The Customer shall ensure that it is entitled to transfer the relevant Service Data to PS Financials Ltd;
2. We will only act on the written instructions of our Customer (unless required by law to act without such instructions);
3. We will ensure that people processing the Service Data are subject to a duty of confidence;
4. We take appropriate measures to ensure the security of processing;
5. We will only engage a sub-processor with the prior agreement of our Customer which is given in the contractual agreement between PS Financials and our Customer;
6. We shall inform the Customer of any intended changes concerning the addition or replacement of sub contracted processors;
7. We will assist our Customer in providing subject access and allowing data subjects to exercise their rights under the GDPR;
8. We will assist our Customer in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessment;
9. We will delete or return all Service Data to our Customer as requested or as stipulated at the end of the contract;
10. We will submit to audits and inspections and provide the controller with whatever information it needs to ensure that we are both meeting the Article 28 obligations and tell the controller immediately if we are asked to do something infringing the GDPR or other data protection law of the EU or a member state;
11. We acknowledge that nothing within our contract relieves us of our own direct responsibilities and liabilities under the GDP;
12. We will co-operate with supervisory authorities (such as the ICO) in accordance with Article 31;
13. We will ensure the security of our processing in accordance with Article 32;
14. We will keep records of our processing activities in accordance with Article 30.2;
15. We will notify any data breaches to the controller in accordance with Article 33;
16. We employ a data protection officer in accordance with Article 37



## PS Financials Service Data

### What is Service Data?

Service Data is any information, including personal data, which is stored in or transmitted via the PS Financials Ltd services, by, or on behalf of, our Customers.

### Who owns and controls Service Data?

From a privacy perspective, the Customer is the controller of Service Data, and PS Financials Ltd is a processor. This means that throughout the time that a Customer subscribes to services with PS Financials Ltd, the Customer retains ownership of and control over Service Data in its account.

### How does PS Financials Ltd use Service Data?

We use Service Data to operate and improve our services, help Customers access and use the services, respond to Customer inquiries, and send communication related to the services.

### What steps does PS Financials Ltd take to secure Service Data?

PS Financials Ltd prioritises data security and combines enterprise-class security features with comprehensive audits of our applications, systems, and networks to ensure Customer and business data is always protected.

For example, PS Financials Ltd servers are hosted at Tier III ISO 27001 compliant facilities. Additionally, we engage third-party security experts to perform detailed penetration tests on a periodic basis, and our Support team is available to respond to security alerts and events.

### Where will Service Data be stored?

PS Financials Ltd data centers are based in the UK.

### How does PS Financials Ltd Respond to Information Requests?

PS Financials Ltd recognises that privacy and data security issues are top priorities for Customers. PS Financials Ltd does not disclose Service Data except as necessary to provide its services to its Customers and comply with the law.

In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. We may disclose personal data to respond to court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims. We may also share such information with relevant law enforcement agencies or public authorities if we believe same to be necessary in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our Terms and Conditions, or as otherwise required by law.



## Data Protection Bill

The Data Protection Bill seeks to empower individuals to take control of their personal data and to support organisations with their lawful processing of personal data.

The Data Protection Bill (Bill) was announced in the Queen's Speech on 21 June 2017. The Bill updates data protection laws in the UK, supplementing the General Data Protection Regulation (EU) 2016/679 (GDPR), implementing the EU Law Enforcement Directive, as well as extending data protection laws to areas which are not covered by the GDPR. It is intended to provide a comprehensive package to protect personal data.

### What is the difference between the DP Bill and the GDPR?

The GDPR has direct effect across all EU member states and has already been passed. This means organisations will still have to comply with this regulation and we will still have to look to the GDPR for most legal obligations. However, the GDPR gives member states limited opportunities to make provisions for how it applies in their country. One element of the DP Bill is the details of these. It is therefore important the GDPR and the Bill are read side by side.

However, the DP Bill is not limited to the UK GDPR provisions.

### What else does the Bill cover?

- The Bill has a part dealing with processing that does not fall within EU law, for example, where it is related to immigration. It applies GDPR standards, but it has been amended to adjust those that would not work in the national context.
- It also has a part that implements the EU's Law Enforcement Directive. This is part of the EU's data protection reform framework and is separate from the GDPR. The Bill has provisions covering those involved in law enforcement processing. The ICO has produced a 12 step guide for preparing for the law enforcement requirements (part 3) of the DP Bill. Our webinar also has helpful guidance on the preparations organisations should be making to prepare for the change in legislation.
- National security is also outside the scope of EU law. The Government has decided that it is important the intelligence services are required to comply with internationally recognised data protection standards, so there are provisions based on Council of Europe Data Protection Convention 108 that apply to them.
- There are also separate parts to cover the ICO and our duties, functions and powers plus the enforcement provisions. The Data Protection Act 1998 is being repealed so it makes the changes necessary to deal with the interaction between FOIA/EIR and the DPA.

The Data Protection Bill key facts can be found here: <https://ico.org.uk/media/for-organisations/documents/2258303/ico-introduction-to-the-data-protection-bill.pdf>



## GDPR

Since our inception, PS Financials Ltd's approach has been anchored with a strong commitment to privacy, security, compliance and transparency. This approach includes supporting our Customers' compliance with UK and EU data protection requirements, including those set out in the General Data Protection Regulation ("GDPR"), which becomes enforceable on May 25, 2018.

If a company collects, transmits, hosts or analyses personal data of EU citizens, GDPR requires the company to use third-party data processors who guarantee their ability to implement the technical and organisational requirements of the GDPR. To further earn our Customers' trust, our contractual agreements has been updated to provide our Customers with contractual commitments regarding our compliance with applicable UK data protection law and to implement additional contractual provisions required by the GDPR. Our contractual commitments guarantee that Customers can:

- Respond to requests from data subjects to correct, amend or delete personal data.
- Be made aware of and report personal data breaches to relevant supervisory authorities and data subjects in accordance with GDPR timeframes.
- Demonstrate their compliance with the GDPR as pertaining to PS Financials Ltd's Services.

### What is the GDPR?

The General Data Protection Regulation ("GDPR") is the new European privacy regulation which will replace the current EU Data Protection Directive ("Directive 95/46/EC"). The GDPR aims to strengthen the security and protection of personal data in the EU and harmonize EU data protection law.

### To whom does the GDPR apply?

The GDPR applies to all organisations operating in the EU and processing "personal identifiable data" of EU residents. Personal data is any information relating to an identified or identifiable natural person.

### What implications does GDPR have for organisations processing the personal data of EU citizens?

One of the key aspects of the GDPR is that it creates consistency across EU member states on how personal data can be processed, used, and exchanged securely. Organisations will need to demonstrate the security of the data they are processing and their compliance with GDPR on a continual basis, by implementing and regularly reviewing robust technical and organisational measures, as well as compliance policies.

### How has PS Financials Ltd been preparing for the GDPR?

PS Financials Ltd will be compliant with the GDPR when it becomes enforceable in May 2018. Our GDPR compliance team is working with Customers to answer their questions and to help them prepare for using PS Financials Ltd's Services after the GDPR becomes effective. Additionally, our GDPR is reviewing PS Financials Ltd's current product features and practices to ensure we support our Customers with their GDPR compliance requirements.

### How can PS Financials Ltd Customers prepare for GDPR enforcement?

PS Financials Ltd encourages Customers to begin preparing for the GDPR by reviewing their privacy and data security processes and policies to ensure compliance by May 2018. Data controllers bear



the primary responsibility for ensuring that their processing of personal data is compliant with EU data protection law. Below are some key points to consider for GDPR compliance:

- **Rights of End-Users:** Organisations should be cognisant of End-Users whose personal data they may be processing. The GDPR establishes enhanced rights for End-Users, and organisations should be able to accommodate those rights.
- **Data Breach Notifications:** Organisations that are controllers of personal data should have clear processes in place in order to comply with the GDPR requirement to report data breaches in accordance with the time frames set out within the GDPR. PS Financials Ltd will notify affected Customers without undue delay if we become aware of a data breach of our services.
- **Appointment of Data Protection Officer (“DPO”):** Customers may need to appoint DPOs to manage issues relating to the processing of personal data.
- **Data Protection Impact Assessment (“DPIA”):** DPIAs usually describe organisations data processes and protective measures, particularly those that may be risky. For data processing activities, Customers need to conduct and file with authorities a DPIA.

PS Financials provides an online training and GDPR compliance monitoring service, which can be found by following this link: - <https://www.gdpr.co.uk/?ref=psfinancials>