



General Data Protection Regulation

Customer/Supplier Privacy Notice

SBA FLIGHT SUPPORT SERVICES LIMITED (“THE COMPANY”, “US”)

1. Introduction

- 1.1. This notice (“Notice”) has been developed to ensure our customers and suppliers feel confident about the privacy and security of personal data and to meet our obligations under the General Data Protection Regulation (“GDPR”) and the Data Protection Acts, 1988 to 2018 (together, the “Legislation”). Under the Legislation, ‘personal data’ is information that identifies you as an individual or is capable of doing so (“Your Data”).
- 1.2. To the extent we as a ‘data controller’, we must comply with the data protection principles set down in the Legislation and this Notice applies to all personal data collected, processed and stored by us in the course of our activities. The purpose of this Notice is to set out the procedures that are to be followed when dealing with personal data and to outline how we will collect and manage personal information in accordance with the Legislation. The procedures set out herein must be followed at all times by us.
- 1.3. This Notice extends to all personal data whether stored in electronic or paper format.

2. How we gather Information

- 2.1. We gather Your Data from when you email us or engage with us or access our website.

3. Scope

- 3.1. This Notice covers the processing by the Company of all ‘personal’ data in relation to data subjects. It applies equally to personal data held in manual or electronic form. Data subjects for the purpose of this Notice include, but are not limited to customers and suppliers.

4. What Personal Information do we hold on customers and suppliers?

- 4.1. We only hold personal data that is directly relevant to our dealings with a given data subject. That data will be collected, held, and processed in accordance with the Legislation and with this Notice in a reasonable and lawful manner.
- 4.2. The customer will be requested to provide the following information for provision of services and for the purposes of billing:
 - personal identification data, including: name, address, phone number and/or email address(es)
 - online identification data, including: IP address
- 4.3. In certain circumstances, we may collect information from you in relation to your employees or workers. For example, passport data for pax and crew visas and other personal data.

5. Why we process Your Data and legal basis for processing

- 5.1. We collect and process personal data relating to our customers in order to ensure that we can provide our services to customers under the terms of the services agreement with the customer, so as to provide the services in the best possible manner and to efficiently manage

our customers as a whole. We use personal data in order to ensure we are able to perform services agreements with customers for the provision of agreed services. We may also use personal data in meeting certain obligations imposed by law.

5.2. We rely on the following legal bases under the Legislation in processing Your Data:

Legal Basis	Example
Consent	We will process Your Data with your consent.
Performance of a contract	We will process Your Data to perform our obligations under your service contract.
Compliance with legal obligations	We may need to disclose Your Data to comply with a request from law enforcement, or other government agencies or court order.
Legitimate interests	To administer your contract and in our business interests.

6. How we may use Your Data

6.1. Business processes or administration uses for Your Data include:

- (direct provision of the services to you;
- resolving issues arising in respect of the provision of the services or the services agreement with you;
- billing for services provided by us under the services agreement with you;
- administration of customer accounts, including: ensuring the ongoing provision of optimized services to you;
- informing you of the status of the services; and
- implementing any changes to services, billing or customer information as requested by you.

6.2. In addition, we may also use personal data gathered from you in relation to your employees as outlined at 4.3 above in order to secure visas, permits, for travel bookings and in generally performing the services. Where we process such data on your behalf, appropriate contractual controls will be entered into governing the collection and use of such data.

7. Security and disclosure of data

7.1. Personal data may be disclosed internally when passed from one department to another in accordance with the data protection principles and this Notice. Personal data is not passed to any internal department or any individual that does not reasonably require access to that personal data with respect to the purpose(s) for which it was collected and is being processed.

7.2. Relevant internal departments to whom personal data may be disclosed are as follows:

- Administration
- Sales
- Billing and accounts

7.3. We shall disclose customer information to third parties only when it is necessary as part of our business practices or when there is a legal or statutory obligation to do. Categories of such third parties may include:

- subcontractors
- credit collection agencies
- auditors
- authorities to whom we are legally obliged to disclose customer information, e.g. law enforcement, tax authorities, etc.

7.4. Whenever we disclose customer information to third parties, we will only disclose that amount of personal information necessary to meet such business need or legal requirement. Third parties that receive customer information from us must satisfy us as to the measures taken to protect the personal data such parties receive.

7.5. Appropriate measures will be taken to ensure that all such disclosures or transfers of customer information to third parties will be completed in a secure manner and pursuant to contractual safeguards.

7.6. We may provide information, when legally obliged to do so and in response to properly made requests, for the purpose of the prevention and detection of crime, and the apprehension or prosecution of offenders. We may also provide information for the purpose of safeguarding national security. In the case of any such disclosure, we will do so only in accordance with the Legislation.

7.7. We may also provide information when required to do so by law, for example under a court order.

7.8. We may also transfer data to legal counsel where same is necessary for the defence of legal claims.

7.9. If there is any change in the ownership of the Company or any of its assets, we may disclose Your Data to the new (or prospective) owner. If we do so, we will require the other party to keep all such information confidential.

8. Retention of data

8.1. The time period for which we retain information varies according to the use of that information. In some cases there are legal requirements to keep data for a minimum period of time. Unless specific legal requirements dictate otherwise, we will retain information no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

- 8.2. Customer personal data will be held for as long as the customer holds a services agreement for the provision of services with us. Following termination of service, customer personal data shall continue to be retained for the minimum period mandatory under local law. Following this mandatory period, personal data shall be retained for no longer than necessary to allow for the defence of legal claims in accordance with applicable statutory limitation periods under local law. Following the expiry of this period customer personal data held by us will be destroyed.
- 8.3. For further information regarding relevant retention periods, you should refer to the Retention Policy, which is attached to this Notice.

9. **Where we store Your Data**

- 9.1. We might store Your Data in different places. Physical files are stored in our office and our archives. Electronic files are stored on our secure servers and in the cloud.

10. **How do we protect data about you when it is transferred out of Europe?**

- 10.1. We may transfer Your Data to, and store it at, a destination outside of the European Economic Area (the "EEA"). Whenever we transfer Your Data in such a way, we will ensure appropriate safeguards are in place.
- 10.2. Your data may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Such staff maybe engaged in, among other things, the processing of your details. Any transfer of Your Data outside of the EEA would only be made through transfer mechanisms approved or allowed for under the Legislation and we shall take all necessary steps to ensure that there is adequate protection, as required by Legislation.

11. **Your rights in respect of Your Data**

- 11.1. You have the following rights in respect of Your Data under the Legislation:

- the right to request from us access to Your Data and to have any incorrect personal data rectified
- in some circumstances, the right to receive some of Your Data in a structured, commonly used and machine-readable format and/or request that we transmit that data to a third party where this is technically feasible but please note that this right only applies to personal data which you have provided to us;
- the right to the restriction of processing concerning you or to object to processing but please note that there may be circumstances in which we are legally entitled to retain Your Data notwithstanding any objection by you to, or request from you to restrict, our processing of Your Data;
- the right to have Your Data erased in circumstances but please note that we may be legally entitled to refuse that request and retain Your Data;
- information on the existence of automated decision-making, if any, as well as meaningful information about the logic involved, its significance and its envisaged consequences.

11.2. We shall employ reasonable means to keep Your Data accurate, complete and up to date in accordance with the purposes for which it was collected.

11.3. You are responsible for ensuring that you inform us at privacy@sba-fss.ie of any changes in Your Data.

12. How can you make a complaint about the use of Your Data

12.1. Complaints on the use, retention and disposal of personal data can be submitted via email to privacy@sba-fss.ie].

12.2. As a customer you also have the right to lodge a complaint with the Data Protection Commission.

13. Changes to Notice

13.1. This Notice will be reviewed from time to time to take into account changes in the law and the experience of the notice in practice. Any and all changes will be advised to employees prior to the date the change becomes effective. We encourage you to periodically review this notice to stay informed about how we collect, use, and disclose personal information.

14. Contact Information

14.1. Questions, comments and requests regarding this notice are welcomed and should be addressed to: privacy@sba-fss.ie

Retention Policy

1 Purpose

1.1. This document outlines the Company's policy concerning the retention of personal data.

1.2. This policy is in compliance with the Data Protection Acts 1988 to 2018, which enact the principles of the General Data Protection Regulation, 2016/679 (GDPR) and in compliance with other legislation, principally various specific employment and safety, health and welfare legislation that outline mandatory time limits for which certain types of customer records must be retained.

2. Scope

2.1. This policy applies only to personal data records held and managed by the Company in either hard copy or electronic format, including records held or being processed by third parties on its behalf.

2.2. All employees of the Company are responsible for the appropriate management of personal data records in accordance with this policy.

3. Policy

3.1. The Company shall apply a retention period to all personal data records. These periods are outlined in the schedule to this policy.

3.2. The retention period for personal data records is the minimum length of time, as documented in the schedule, that a personal data record must be retained. Retention periods can vary because of the content of records. Some records are significant enough to be retained for a long period, while other records have a shorter retention period. The rationale for applying a retention period is typically based on operational or legal requirements.

3.3. A retention period of 'permanent' should not be applied to records unless retention of those records for an indefinite period is necessary for the purpose of discharging any of the Company's functions or purposes. 3.4. Personal data records may be kept beyond their defined retention period if the data is anonymised such that the data may no longer be attributed to a specific data subject.

3.5. Personal data records should be destroyed after their retention period has expired. For electronic personal data records, this should be done via secure deletion or the physical destruction of CDs or USB keys. Hard copy records should be shredded/destroyed using secure methods.

4. Definitions

1. Retention is defined as the maintenance of records in an environment that can be assessed by authorised users.
2. Destruction is defined as the physical or technical destruction sufficient to render the information contained in the record irretrievable (i.e. put beyond use).

SCHEDULE 1

Minimum Retention Periods

Table 1 outlines the principal statutory and commercial records requirements. **Note that not all of these categories of data might apply to all Companies**

Table 1: Principal Statutory & Commercial Records/Documents

Record Type	Minimum Retention Period
Register of Members	Permanent or until company is dissolved
Minutes of proceedings of meetings of Company Permanent and Directors	Permanent
Statutory Books	Permanent
Share Registration Documents	Permanent
Commercial Contracts/License Agreements Guarantees <ul style="list-style-type: none"> ✓ Security Documentation ✓ Financial Documentation ✓ Loan Documentation ✓ Title Documents 	Length of legal relationship plus 6 years from end of current financial year
Documents relating to Property: <ul style="list-style-type: none"> ✓ Deeds of title relating to freehold property ✓ Leases ✓ Planning Permissions ✓ Agreements with architects and builders 	<ul style="list-style-type: none"> Until disposal of property plus 12 years Until disposal or 12 years after termination 12 years after Interest in property ceases 6 years after completion of contract

Books of Account :	Termination plus 6 years from end of current financial year
<ul style="list-style-type: none"> ✓ Annual Accounts ✓ Quarter Close ✓ Monthly Management Accounts ✓ Weekly Management Accounts ✓ Weekly Treasury Reports 	
Third Party Guarantees:	Termination plus 6 years
<ul style="list-style-type: none"> ✓ Letters of credit ✓ Letters of guarantee 	Termination plus 12 years
Audit Certificates	Termination plus 6 years
Tax Files	6 Years after the end of the financial year of termination
Vat Files	6 Years after the end of the financial year of termination
HR: General Personnel (HR) Records, including training records, contract of employment, employment particulars of employment and changes to terms and conditions of employment	7 Years following the end of the period of employment
HR: Applications for employment and interview records of unsuccessful candidates	18 months from once all candidates have been advised of the outcome of the process.
HR: PAYE Records	6 Years following the end of the tax year to which they relate
HR: Employee Bank Records	6 months following the end of the period of employment
HR: Annual Leave Records	3 Years following the end of the period of employment
HR: Working Hour Records	7 Years following the end of the period of employment
HR: Sick Leave Pay Records	7 Years following the end of the period of employment
HR: Maternity Records	7 Years following the end of the tax year in which the maternity pay period ends
HR: Paternity and Parental Leave Records	8 Years following the end of the tax year in which the paternity and parental leave period ends
HR: Work Permits and Visas	5 Years or if the non-EEA national remains in the employment for longer than 5 years from the date of the permit, then for the entire period of employment
Records contained in the Register of young persons as required by s.15 of the protection of young Persons (Employment) Act , 1996	3 Years after the young person reached their 18 th birthday

HR : Pension Records	Permanently
HR : Death benefit nomination and revocation forms	Periods of employment or 6 years after payment of benefit, as the case may be
HR : Consent for the processing of personal and sensitive data	For as long as the data is kept plus 7 years
Consumer Records : Online Shopping, loyalty , Focus Groups Competitions and mobile apps	2 Years from the last Interaction
Accident Reports	10 Years

Additional Definitions and Definition information

Data is recorded information whether stored electronically, on a computer, or in certain paper-based filing systems.

Data protection principles mean the legal conditions for processing personal data.

Data subjects for the purpose of this policy, include all living individuals about whom the Company holds personal data. A data subject need not be an EU national or resident. All data subjects have legal rights in relation to their personal information.

According to the Data Protection Commissioner's website, Personal data means data that relate to a living individual who can be identified:

- (a) from those data, or
- (b) from those data and other information that is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the Individual. It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data".

Data controllers are the people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. The Company is the data controller of all personal data used in its business.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which process personal data on the Company's behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

REFERENCES

<https://www.dataprotection.ie>

http://www.citizensinformation.ie/en/government_in_ireland/national_government/standards_and_accountability/data_protection.html

