Steinhoff UK Beds Limited
Data Protection Policy

Last updated: May 2018
Version: 1
Document owner: Legal

1. Background

1.1 Data protection laws give people legal rights regarding how their personal data is processed. These rights apply to you, as well as to every individual whose personal data you process while working for us.

1.2 Steinhoff UK Beds Limited ("**Steinhoff UK Beds**", "**we**", "**us**" or "**our**") have obligations under these data protection laws regarding how we treat the personal data we hold, what we do with it and who we share it with. We take these obligations seriously and we consider them as critical to our business.

2. What is this policy and why do you need to read it?

2.1 This policy sets out:

2.1.1 details of our legal obligations in relation to personal data; and

2.1.2 what your responsibilities are to ensure that we comply with them.

2.2 Everyone who works for us, whether as our employee or in another capacity as part of our business operations, must comply with this policy when processing personal data. In this policy references to "**you**" mean anyone that processes personal data for us, regardless of their employment status.

2.3 This policy applies whenever you handle personal data about anyone else, including colleagues, job applicants, customers and suppliers who are individuals or partnerships and individuals at customers and suppliers that are companies.

2.4 You have a responsibility to read and comply with this policy and any other policies referred to in it, as well as to attend all mandatory data protection training that we provide to you. It is important that you understand what is required of you. Data protection is a serious matter and failure to comply with this policy may lead to disciplinary action which could result in summary dismissal.

2.5 Data protection legislation is enforced in the UK by the **Information Commissioner's Office**, who can investigate complaints, audit our use of personal data and take action against us (and in some cases against you personally) for breach of this legislation. Enforcement action may include fines, criminal prosecution and preventing us from using personal data, which could prevent us from carrying on our business.

2.6 If we breach data protection legislation we could also have compensation claims made against us by individuals who are affected.

2.7 We have appointed a Compliance Team at GDPR@steinhoff.co.uk whose role is to inform and advise us about, and to ensure that we remain compliant with, data protection legislation. This person should be your first point of contact if you have any queries or concerns about this policy or about dealing with personal data.

3. Key terms used in this policy

3.1 "**Personal data**" is information (in any format) that relates to a living individual who can be identified from that information, either on its own or when it's combined with other information held by us.

3.1.1 For example, names, addresses, contact details, salary details, job titles, CVs, CCTV images, credit card numbers, logon credentials, marketing preferences and data gathered from website cookies are all capable of being personal data.

3.1.2 When considering whether data allows an individual to be identified you should think about it as a jigsaw piece and ask yourself whether if you were to put it together with all the other jigsaw pieces that we hold it would be possible to identify an individual.

3.1.3 As you can see, the definition is broad, and increasingly – as technology enables us to identify individuals more easily – more data is likely to be regarded as personal data.

3.2 In this policy we refer to "processing" personal data. "**Processing**" means any activity carried out in relation to personal data, including collecting, recording, organising, storing, retrieving, altering, using, disclosing and destroying personal data.

3.3 "**Data subject**" is a term used in data protection legislation – it means the individual to whom the personal data relates. For simplicity, in this policy, we sometimes refer to these people as 'individuals'.

3.4 "**Special personal data**" (sometimes referred to as sensitive personal data or special category data) is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data (where it's processed to uniquely identify someone), data concerning health or someone's sex life or sexual orientation.

4. Data protection principles

4.1 There are six main principles, which we must follow in respect of all personal data we process. It is essential that you also comply with them when processing personal data for us.

4.2 The principles are that personal data must be:

4.2.1 processed lawfully, fairly and in a transparent manner (see **paragraph 4.3**).

4.2.2 processed only for the specified, explicit and legitimate purpose(s) we collect it for (see **paragraph 6**).

4.2.3 adequate, relevant and limited to what we need in relation to the purpose(s) we collect it for (see **paragraph 8**).

4.2.4 kept accurate and kept up to date (see **paragraph 9**).

4.2.5 kept for no longer than necessary in relation to the purpose(s) we process it (see **paragraph 10**).

4.2.6 kept secure (see **paragraph 11**).

4.3 We may be asked to demonstrate that we have complied with the data protection principles at any time. Therefore, part of your role is therefore to ensure that you make a record of any personal data that you process and how the processing complies with those principles.

5. Lawfulness, fairness and transparency

5.1 We must always have a "**lawful basis**" for processing personal data. The lawful bases which are most likely to be relevant to our processing are where:

5.1.1 the individual has given his or her **consent** to the processing.

> **NOTE**:
> - Consent must be a freely given, specific, informed and unambiguous indication of the individual's wishes in order to be valid. This means that the use of pre-ticked tick boxes (or other methods which assume that silence constitutes consent) will not be sufficient.
> - Where the individual is asked to give a written declaration of consent, the request should be clearly distinguishable from other matters and in an intelligible and easily accessible form, using clear and plain language.
> - Individuals can withdraw their consent at any time (see **paragraph 14.1.8**) and we have to make sure it's easy for them to do so.

5.1.2 the processing of the individual's personal data is **necessary to perform a contract** with that individual or to take steps at the request of the individual before entering into a contract.

5.1.3 the processing is **necessary to comply with a legal obligation** to which we are subject.

5.1.4 the processing is **necessary in order to protect the vital interests** of an individual.

5.1.5 the processing is **necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in us.

5.1.6 the processing is **necessary for our legitimate interests**, provided those interests are not overridden by the individual's interests, rights or freedoms.

> **NOTE**:
> - Individuals have a right to object to our processing of their personal data where we are relying on this lawful basis for that processing (see **paragraph 14.1.7.2**).
> - We must make sure that we let people know when we are relying on this lawful basis for any processing of their personal data (see **paragraph 5.2**).

5.2 We must give individuals very specific information about how we process their personal data, to ensure that our processing is **fair and transparent**. This information is often referred to as a fair processing notice or privacy notice.

> **NOTE**:
> - You should contact our Compliance Team at GDPR@steinhoff.co.uk to discuss your fair processing notice requirements before collecting any personal data in connection with any projects, products or services you are designing, offering or providing.
> - We should provide the information in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
> - In most circumstances, we should provide the information at the time the individual's personal data is collected.

We have set out below the procedures you should follow in respect of each channel by which we collect personal data:

5.2.1 **Our websites and other digital platforms**. You should make sure that the relevant website or digital platform contains a permanently visible link to our online Privacy Policy.

5.2.2 **In store and other offline channels.** You should implement our fair processing notice and ensure that it can be provided to data subjects in store / by phone in line with our stated procedures.

6. Special personal data

6.1 An extra layer of rules apply when we process special personal data.

6.2 We still need to have a lawful basis (as referred to in **paragraph 4.3**) for processing special personal data, but we also need an additional justification for processing it. The justifications that are most likely to be relevant are:

6.2.1 where the individual has given their explicit consent to the processing, or

6.2.2 where the processing is necessary for employment or social security purposes (**NB** This policy is also our policy for the purpose of Part 4 of Schedule 1 of the Data Protection Act 2018).

> ✎ **NOTE**:
> You must take extra care when you process special personal data because of the potential for harm or distress if it is received by an unintended recipient or if it goes astray. Therefore, you should not email it or disclose it unless you take steps to encrypt or otherwise secure it.

6.3 If you have any questions or concerns in relation to processing special personal data, you should contact our Compliance Team at GDPR@steinhoff.co.uk.

7. Purposes for processing personal data

You should only process personal data that is necessary for a legitimate business purpose that is communicated to the individual (in line with **paragraph 5.2**) and it mustn't be further processed for reasons which aren't compatible with those purposes.

8. Adequate, relevant and necessary personal data

You should consider carefully how much personal data you actually need for the legitimate business purpose(s) you have identified for your processing activity. Do not collect personal data that is just "nice to have". It should only be the minimum necessary for the purpose.

9. Keeping personal data accurate

9.1 We must keep personal data accurate – and every reasonable step must be taken to erase or rectify inaccurate personal data. The best way to help us do this is to check with the individual that their personal data is correct at the time it is collected.

9.2 In order to ensure that personal data is kept up to date, you should ask the individual whether there have been any changes to their personal data each time you contact them.

9.3 You must update personal data with all necessary changes as soon as you become aware that it is inaccurate or out of date, and ensure that the updates are made across all relevant records and systems.

10. Retaining personal data

10.1 We can only keep personal data in a form which permits us to identify the individual concerned for as long as is necessary for the purpose(s) for which it has been collected. Even greater care needs to be taken to ensure that special personal data is not retained for longer than is necessary.

10.2 Please refer to our customer and employee privacy notices for more information our retention periods.

11. Security of personal data

11.1 We are required by law to have appropriate technical and organisational security measures in place to prevent unauthorised or unlawful processing and accidental loss or destruction of or damage to personal data. We may have to report any threat to or breach of security to the Information Commissioner's Office and to any affected data subjects.

11.2 We need everyone's help to keep personal data secure and everyone shares responsibility for this. You should help us do this by:

11.2.1 complying with our IT and information security policies;

11.2.2 considering carefully what format (eg paper or electronic) is required for the personal data you are processing;

11.2.3 using common-sense, practical measures to protect the security of personal data (and in particular special personal data);

> **NOTE**:
> For example:
> - you must only access personal data to the extent you need it to perform your role;
> - if you need to use paper records ensure that they are stored in a safe place when not in use and dispose of them in confidential shredding bins once they are no longer required;
> - do not leave printing containing personal data on printers;
> - lock your screen when you are away from your desk;
> - never share passwords or login details with others; and
> - ensure that others cannot read the information on your screen over your shoulder.

11.2.4 before sending an email – pausing and checking that the content, attachments/enclosures and addresses/recipients are correct and that the email will be sent only to the people it's intended for;

11.2.5 not sharing personal data with anybody (including people within our business) unless you are sure who they are and why they need access to the relevant personal data; and

11.2.6 ensuring the ongoing confidentiality, integrity, availability and resilience of the systems processing systems and services we use for processing personal data.

11.3 You must only use the personal data of others which you have access to in the performance of your role for our business purposes. You must not misuse it, for example by using the data for your own purposes, or those of family or friends, or disclosing it to others to use for their purposes. This would be a breach of our data security rules. It could be a breach of applicable data protection laws and indeed be a criminal offence in some cases.

12. Dealing with personal data breaches

12.1 A "**personal data breach**" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It covers malicious incidents such as a cyber-attack, but it also covers other incidents many of which can arise as a result of human error. For example, a lost laptop, device or file or giving personal data to the wrong person over the telephone or via email.

12.2 If you discover or suspect that there is or has been a security breach, you must inform our Compliance Team at GDPR@steinhoff.co.uk. It is important that you do this **immediately** as we are required by law to deal with personal data breaches within very strict timescales.

13. Sharing personal data with other people

13.1 Third parties (ie companies, businesses or people outside Steinhoff UK Beds) may need to access the personal data we process, for example as part of providing services to us. However, we are only permitted to disclose personal data to third parties in certain limited circumstances.

13.2 When we are considering engaging a supplier outside of Steinhoff UK Beds to process personal data on our behalf (a "**third party supplier**"), we must always have regard to the following:

13.2.1 **Due diligence** - we must select a third party service provider who provides sufficient guarantees with respect to data security and the handling of personal data generally.

13.2.2 **Contractual obligations** - we must ensure that there is a written contract in place with the third party service provider which includes specific data privacy obligations protecting personal data. Therefore, always check with Group Legal before sharing any personal data with a third party service provider.

13.2.3 **Compliance monitoring** - we must take reasonable steps to monitor the third party service provider's performance of the relevant security and processing obligations.

13.2.4 **International transfers** - if engaging a third party service provider will or may involve personal data being processed abroad or overseas, additional data protection and privacy considerations must be addressed and this generally means that additional clauses must be included in the contract.

13.3 We must never disclose personal data outside Steinhoff UK Beds to anyone other than a third party supplier (see **paragraph 13.2**) except where this is lawful, including where it is necessary:

13.3.1 to protect an individual's vital interests;

13.3.2 to comply with a law, regulation or court order, for example, where requested by customs officials for the investigation of tax offences;

13.3.3 to respond to any legitimate request for assistance by the police or other law enforcement agency;

13.3.4 to engage and/or obtain advice from professional advisers (eg accountants, lawyers, external auditors etc);

13.3.5 to deal with any legal dispute or administrative claim between us and a third party (eg to that third party and lawyers representing them);

13.3.6 to liaise with potential buyers or other third parties in connection with the disposal of or merging of any Steinhoff UK Beds asset(s) or entity/(ies); or

13.3.7 as otherwise permitted by, and in accordance with, applicable laws.

13.4 You should always check with our Compliance Team at GDPR@steinhoff.co.uk if you are unsure whether or not you are permitted to disclose personal data to a third party.

14. Individuals' rights in relation to their personal data

14.1 Individuals have the following legal rights in relation to their personal data:

14.1.1 **Right to information** – See **paragraph 5.2**;

14.1.2 **Right of access** – Individuals are entitled to receive confirmation from us as to whether or not we are processing personal data about them and, if we are, to access it and be provided with certain information in relation to it, such as the purpose(s) for which it is processed, the persons to whom it is disclosed and the period for which it will be stored;

14.1.3 **Right to rectification** – Individuals can require us to correct any inaccuracies without undue delay;

14.1.4 **Right to erasure** (also known as the right to be forgotten) – Individuals can require us to erase their personal data, without undue delay, if we no longer need it for the purpose for which we have it or if it is being unlawfully processed or if erasure is required to comply with a legal obligation to which we are subject. There are some exceptions to this right;

14.1.5 **Right to restriction of processing** – Individuals can require us to restrict processing in certain circumstances including if the personal data is inaccurate or if the processing is unlawful;

14.1.6 **Right to data portability** – Individuals can, in certain circumstances, receive the personal data in a structured, commonly used and machine-readable format so that it can be transferred to another provider; and

14.1.7 **Right to object** – Individuals can object to:

14.1.7.1 any decision we make which is based solely on "automated processing" (ie without any human involvement) (**NB** There are some limits and exceptions to this right); and

14.1.7.2 us processing their personal data where we are relying on the lawful basis that our processing is necessary for a legitimate interest.

14.1.8 **Right to withdraw consent** – Individuals have the right to withdraw their consent to our processing of their personal data at any time. If this happens, we must stop processing their personal data unless there is another lawful basis we can rely on – in which case, we must let the individual know. (**NB** If someone withdraws their consent, it won't impact any of our processing up to that point.)

15. Dealing with communications in relation to personal data

15.1 If you receive any communication from an individual in relation to their personal data or from any other person or body (including the Information Commissioner's Office) in relation to personal data, you must inform our Compliance Team at GDPR@steinhoff.co.uk immediately, and provide details of the relevant communication.

15.2 We have to respond to certain requests from individuals in relation to their personal data within strict timescales, so it is very important that our Compliance Team is made aware of each request **as quickly as possible**. You must also cooperate with that team by providing any other information and assistance that they may require.

15.3 **Please do not, under any circumstances, respond to requests or communications about personal data yourself without input from our Compliance Team at GDPR@steinhoff.co.uk.**

16. Personal data and direct marketing

16.1 There are strict laws which govern direct marketing practices (in addition to data protection legislation). For example, we may need to obtain the individual's explicit consent (for example, by way of an opt-in tick box) before we can send them electronic marketing communications. Therefore, please contact our Compliance Team at GDPR@steinhoff.co.uk before you send out any marketing communications.

16.2 In any event, as a matter of good practice, you should:

16.2.1 never buy or sell marketing lists from or to third parties; and

16.2.2 always provide individuals with a simple means of unsubscribing from (or opting out of) our marketing communications, in every communication we send.