the7stars UK Ltd - Data Protection Policy

Introduction

the7stars has a responsibility to look after the information which we collect about individuals, whether our employees, clients, business partners, as well as any consumer personal data we might process for our own purposes (e.g. research fieldwork).

When people trust us with their information, we should live up to that trust.

Data protection law gives individuals the right to understand – and in some cases control – how their data is used. It also places obligations on us to handle people's data fairly and respect their rights. We take our obligations under data protection law seriously. A breach of our data protection responsibilities could result in a significant financial penalty against us, as well as negative publicity and damage to our brands.

If you have any questions about this Policy, you should contact the7stars directly: Floors 6-8 Melbourne House, 46 Aldwych, London WC2B 4LL or email privacy@the7stars.co.uk

1. Who and What is covered by this Policy?

This Data Protection Policy together with the other policies referred to below should be read and followed by all staff. This Policy applies to all our business units, operations, functions and staff, including permanent and temporary employees and any third party personnel such as agents, temps, contractors and consultants, who have access to ***"personal data"*** which is ***"processed"*** by our agency when we are the ***"data controller"*** *(as opposed to the* ***"data processor"****)*. See below for more details regarding what these terms mean. Any staff who fail to comply with this Policy and the other policies referred to below may be subject to disciplinary action, up to and including dismissal.

What is "personal data"?

This Policy only applies to "**personal data**". This means information which relates to an identified or identifiable individual (i.e. a living person). It includes names, addresses, email addresses, job applications, photographs, and correspondence to and from an individual. Where it can be linked to an individual, it also includes online identifiers and web browsing information (e.g. cookie data).

Note that this Policy does not apply to confidential commercial information which is not personal data, e.g. financial information.

What is "sensitive personal data" (and why is it important)?

Certain personal data is designated as "**sensitive**" and given enhanced legal protection. Sensitive personal data is personal data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; biometric or genetic information; or information about a person's health, sex life or sexual orientation.

What is "processing"?

This Policy also refers to "**processing**" personal data. Processing essentially means doing anything with personal data; this includes collecting it, storing it, combining it with other data, sharing it with a third party, and even deleting it.

We process personal data captured by this Policy when we collect and store data about our own staff, job applicants, staff at our suppliers and our clients, and potentially consumers when we collect and use data for our own purposes (such as when we build our own proprietary agency database). All of this personal data should be treated in accordance with this Policy.

What is a data controller and a data processor?

As mentioned above, this Policy only applies in respect of personal data for which we are the "data controller", and **not** a "data processor".

Broadly speaking, a data controller is the organisation which determines the "purposes" for which and the "manner in which" personal data are processed – i.e. the organisation which decides "why" and "how" personal data are processed. A data processor on the other hand, is an organisation which merely processes personal data "on behalf of" a controller.

We will generally be a **data controller** whenever we process personal data for our own purposes, such as the data of our staff and the staff of our business partners and clients as well as consumer personal data when we process it for our own purposes (such as when we build our own proprietary databases). We will generally be a **data processor** when we process personal data solely on a client's behalf (such as when we run a retargeting campaign for a particular client).

The data controller is responsible for ensuring that the processing complies with data protection law – this includes where the personal data is processed by a service provider which the data controller has appointed to process personal data on the data controller's behalf. It is therefore very important that when we appoint a service provider to process any personal data on our behalf, we put in place a robust contract with the service provider including appropriate data protection clauses. See our **Supplier Contract Guidance** for more details about putting in place contracts with suppliers who will be processing personal data for us.

Where we are a data processor acting on our client's behalf, even though the principles set out below in this policy do not directly apply to us, there **is** a legal requirement to include in our contract with our clients an obligation to assist the client with certain of the client's data protection obligations. It is therefore helpful to understand the principles in this policy as it will help you to understand why the client may have certain expectations regarding data protection.

2. Our Data Protection Principles

Everyone to whom this policy applies should follow our Data Protection Principles when processing personal data for which we are the data controller.

1. **Fairness and Transparency:** Give people information about how we process their personal data.

What does this mean in practice?

We should be transparent and give people information about how we use their personal data. This also means not doing anything with their personal data which they would not expect or that we would be embarrassed for them to know about.

In particular, we should always tell people if their personal data will be passed to a third party. Similarly, if we receive personal data about someone from a third party, we should make sure the individual knows about it as soon we can.

2. Lawful Processing: Make sure we always have a good, lawful reason to process people's personal data.

What does this mean in practice?

We must comply with any applicable laws when we process personal data.

Additionally, we should only process personal data if it can satisfy certain conditions set out in data protection law. The most important of these for us will be one of the following: (i) the relevant individual has given her/his consent; (ii) the processing is necessary as part of a contract with the individual; (iii) the processing is necessary to comply with a legal obligation; or (iv) the processing is necessary for our (or a third party's) 'legitimate interests', provided such interests are not overridden by any risk or harm to the individual.

We should only process sensitive personal data in exceptional circumstances, where we are satisfied we have a lawful basis for doing so.

3. Purpose Limitation: Only collect personal data for a specific purpose. If we want to reuse the personal data for a new purpose, we must make sure the new purpose is compatible with the original purpose.

What does this mean in practice?

We should always have a clear purpose for any personal data before we collect it, and this should reflect a specific business need.

If we later want to use the personal data for a new purpose or share it with a new third party, we should consider whether it is compatible with the original purpose, and whether it would be within the reasonable expectations of the individual to whom the personal data relate.

Before starting any new processing or collecting any new data, you should speak to [Insert relevant agency contact], to ensure data protection and privacy is considered from the outset. If there could be risks associated with any new processing, we may need to conduct a "Data Protection Impact Assessment" ("DPIA") to decide whether any safeguards need to be put in place to protect the individuals. See our **Data Protection Impact Assessment Policy** for more details regarding when and how to carry out a DPIA.

4. Data Minimisation: Only process as much personal data as we need, and no more.

What does this mean in practice?

In any particular case, we should only collect or otherwise process as much personal data as we need for that specific purpose. This means we should not collect personal data that we do not need, or ask for personal data 'just in case' it may be useful.

Before asking for or accessing information about someone, you should ask yourself whether you really need that information to achieve your result.

5. Accuracy: Keep personal data accurate, complete and up-to-date.

What does this mean in practice?

Wherever possible, we should give individuals the opportunity to amend or correct their personal data (and offer a self-service tool where possible). If we become aware of personal data which is inaccurate or out-of-date, we should take reasonable steps to correct it or delete it.

All staff should inform [HR] about any changes in the personal data which we process about them.

6. Retention: Only keep personal data for as long as we need it. If we don't need the personal data anymore, we must delete it or anonymise it.

What does this mean in practice?

We should only keep personal data for as long as we need it for its specified purpose. Once the personal data is no longer needed, it should be deleted, or anonymised so that individuals can no longer be identified from it.

All staff should comply with our **Data Retention Policy**.

7. **Security:** Protect personal data from getting lost or stolen. Make sure our service providers protect our personal data as well.

What does this mean in practice?

We must make sure we always protect personal data with appropriate security measures, to prevent any accidental or unauthorised access, damage, loss or disclosure.

If you become aware of any actual or suspected loss or breach of security relating to personal data, you should refer to our **Data Incident Policy.**

This Security Principle extends to our service providers who handle personal data on our behalf. We should only appoint service providers who can provide appropriate protection for our personal data. You should consult [Insert relevant agency contact] before appointing any service provider who will have access to our personal data or process any personal data on our behalf. You should also look at our **Supplier Contract Guidance** for more details about putting in place contracts with suppliers who will be processing personal data for us.

8. Individual Rights: Allow individuals the right to access, correct or erase their personal data, or object to it being used for certain purposes.

What does this mean in practice?

Anyone whose personal data we process has the right to obtain a copy of that personal data, and correct any inaccuracies. In certain circumstances, they also have a right to have their personal data erased or not used for a particular purpose. For example, individuals have a right to object to decisions being made about them which are solely automated and which

have a significant impact on them (for example a decision to hire an individual based purely on an automated process).

We must respect these rights, and respond to requests in accordance with our legal obligations. We are also entitled to refuse requests in certain circumstances.

If you receive a request from an individual relating to their personal data, please refer to our **Individual Rights Policy**.

9. Personal Data Transfers: Put in place safeguards before sending personal data outside Europe or the UK.

What does this mean in practice?

Because data protection standards may not be the same in countries outside the European Economic Area (**EEA**), UK and EU data protection law places restrictions on when personal data may be transferred outside the UK or the EEA. The transfer will only be allowed if certain safeguards are put in place to protect the personal data, wherever it goes.

These restrictions apply whether we are sending personal data to a third party (e.g. a US-based service provider) [or even a company within our group of companies]. Importantly, the restrictions apply not only when the personal data will be stored in the non-EEA/UK country, but also if the personal data will only be "accessed" remotely from that country (e.g. if they will have access to personal data on our systems).

You should consult [Insert relevant agency contact] before sending personal data outside the EEA/UK or allowing a party outside the EEA/UK to have access to personal data stored within the EEA/UK.

10. Accountability: We will take steps to make sure our processing of personal data complies with this Policy.

What does this mean in practice?

We are responsible for ensuring our processing of personal data is compliant with the law. That is why we have implemented this Data Protection Policy, as well as the various other policies which accompany it. See our list of our other **data protection policies**.

We will conduct training for all staff who handle personal data on their responsibilities under this Policy. It is the responsibility of everyone working at our agency to complete their required training.

Any new websites, apps, or other tools should be designed to enable us to comply with our Data Protection Principles.

We will appoint a Data Protection working team, who will assist with the application of this Policy and any data protection queries. See **[here]** for a full list of the Data Protection working team members.

This Policy and the accompanying policies will be periodically reviewed and updated as necessary to ensure they are effective and meet our requirements.

.

This Policy was last updated on: 12th March 2018