GDPR Case Study

TAYLOR WALTON SOLICITORS

Fictional company: Sky Blue Sports

Sky Blue Sports (**SBS**) sells sports equipment and sports-related products to customers in the UK. SBS is aware that, in May 2018, the General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 introduced changes to the way it can process personal data (**data**).

However, SBS never got around to doing anything about this and is concerned that it may not currently be compliant with this legislation.

Our initial recommendation is for SBS to carry out a full data audit in order to ascertain what data it collects (and how), how it uses this data and what ultimately happens to the data (including transfer to third parties).

Personal data means any information relating to an identified or identifiable natural person, which nearly all organisations are likely to collect.

Data audit outcome

SBS collects customer data by telephone, email and website correspondence. This includes the customer's name, address, phone number, email address, date of birth and nationality. It also collects bank details when processing orders using secure, encrypted technology.

The data is processed by SBS:

(a) By storing it (retention of data constitutes processing for the purposes of the GDPR).

(b) By using it in order to process and deliver customer orders (including payment).

(c) For marketing purposes.

The data is retained indefinitely by SBS unless a customer requests that it is deleted.

SBS also processes data in respect of its own employees, but guidance regarding GDPR implications in respect of employees is outside the scope of this case study.

Questions:

1. A key principle of the GDPR is that SBS must limit the data it collects to what is actually necessary for its purposes. Is all the data SBS collects necessary for its purposes?

2. A key principle of the GDPR is that SBS must keep data for no longer than is necessary for its purposes. Is SBS permitted to retain data indefinitely, barring customer requests?

Answers:

1. The customer's name, address, phone number, email address are likely to be necessary/ useful in processing the order, as are the bank details. It may be harder for SBS to justify collecting the customer's date of birth and nationality, assuming that this is not necessary in connection with SBS's marketing.

2. SBS may only retain data for as long as it has a lawful justification for doing so. Once SBS has fulfilled a customer's order, SBS cannot market to the customer indefinitely.
   SBS may retain (but not otherwise use) the data where it has a legal obligation or right to do so (for example, in connection with possible legal claims). Many commentators have suggested a maximum retention period of 6/ 7 years is appropriate in line with common limitation periods but a longer period may be suitable in certain cases.

Lawful basis

SBS must have justification (a "lawful basis") for each element of its processing of data. Overall, SBS is likely to use several different lawful bases for different types of processing, but it is important for SBS to be able to demonstrate which one lawful basis it uses for each separate type of processing.

There are six lawful bases under the GDPR for processing data, which are essentially:

1. The data subject has given his/ her consent.
2. Processing is necessary for the performance of a contract with the data subject.
3. Processing is necessary for compliance with a legal obligation.
4. Processing is in the data subject's vital interests (life or death situations).
5. Processing is necessary for the performance of a task in the public interest or in exercising official authority/ administering justice (broadly, public authority processing).
6. Processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party

Questions:

1. What is SBS's lawful basis for using data to in order to fulfil customer orders?

2. What is SBS's lawful basis for storing data (say, for 7 years)?

3. What is SBS's lawful basis for using data for marketing purposes?

Answers:

1. As for many organisations, using data to fulfil a customer order is likely to be necessary for the performance of a contract with the data subject.

2. As mentioned above, SBS may justify retaining data for 7 years on the basis that it is necessary to comply with a legal obligation (or meet possible legal claims). However, it should still seek to minimise (streamline) the information which is kept for that purpose.

3. It is likely that SBS would seek to justify marketing to the client on one of the following two lawful bases:
   (a) The data subject has given his/ her consent; or

   (b) Marketing is necessary for the purposes of legitimate interests pursued by SBS.

Marketing

Informing the customer in a transparent manner about SBS's data processing (through an accurate and up to date Privacy Notice or Privacy Policy) is essential whatever lawful bases are used in connection with its processing.

However, as SBS uses the data to carry out marketing, there are additional requirements for it to fulfil, depending on whether it is justifying such marketing through the lawful basis of consent or through the lawful basis of legitimate interests.

It is also important to note that SBS cannot continue to market indefinitely to customers who have not purchased or shown any active interest in SBS's products for some time. The recommended timescale will vary depending on the full context and guidance/ evolving case law, but eventually a customer will become "dormant" and must not be sent marketing material (although SBS may be entitled to retain the data for longer, in case of legal claims).

Where electronic marketing is carried out, SBS must also ensure that it complies with the Privacy and Electronic Communications (EC Directive) Regulations 2003, which is outside the scope of this case study.

Consent

If SBS is using consent as its lawful basis for marketing, it must be able to demonstrate that such consent was freely given, specific, informed and unambiguous. The customer must also be able to easily withdraw consent at any time.

A key change introduced by the GDPR is that a clear affirmative action on the part of the customer is required, so pre-ticked "opt-in" boxes do not constitute valid consent for the purposes of the GDPR.

Legitimate Interests

If SBS is using legitimate interests as its lawful basis for marketing, it must be able to demonstrate that the processing is necessary for the purposes of its legitimate interests and that these are not overridden by the interests or the fundamental rights and freedoms of the customer.

This is not a rubber-stamping exercise. We recommend that a three-stage "legitimate interests assessment" is carried out and carefully documented which demonstrates that, having taking all relevant contextual factors into account, SBS is satisfied that:

1. A legitimate interest exists in this case;
2. The marketing is necessary to achieve the legitimate interest; and
3. SBS's interest is justified when balanced against the data subject's rights and freedoms.

Final thoughts

Establishing a lawful basis for each separate type of processing and documenting this in a Privacy Notice or Privacy Policy (and other documents, where consent or legitimate interests is relevant) is just one part of the GDPR picture. SBS should also consider carefully:

1. The GDPR requirement that all data be processed in a manner that ensures appropriate security of the data.

2. The GDPR requirement that specific contractual obligations are included in contracts between a data controller and each of its data processors (for example, this may be relevant in relation to SBS's IT provider, HR and payroll outsourcing and payment processing).

3. Additional GDPR requirements in relation to special data (for example, data which could reveal an individual's racial or ethnic origin, political opinions or religious and philosophical beliefs, or genetic or biometric data).