

3rd Party Privacy Due Diligence

I. Will Your Company be processing Personal Data*
on behalf of DS Smith

Yes No

II. Personal Data Processing Details (*Complete this section only if the answer to Question I is "Yes"*)

1. Will you use third parties to help deliver these services?

Yes No

2. Will the DS Smith related Personal Data be transferred or accessed from different countries (including through any sub processors)

Yes No

3. Will you process Personal Data involving any of the following? (select all that apply)

a) **Automated decision making with legal or similar effects**

Making automated decisions means the ability to make decisions by technological means without any human involvement. Examples of this include automatic processing which leads to a decision that prevents an individual from accessing a particular product or service.

b) **Profiling**

Profiling means an activity focused on the use of Personal Data to evaluate certain personal aspects relating to a person, to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements. For example, this includes creating marketing profiles on how someone interacts with a website.

c) **Systematic monitoring of individuals**

Systematic monitoring includes activities such as the use of CCTV systems in public spaces and any other regular observation of publicly accessible areas, as individuals are unable to avoid being monitored. It also includes monitoring of employee workstations and internet use at work, as well as monitoring how people use certain services such as tracking driving behaviour.

d) **Combining Personal Data**

Combining or matching Personal Data from two or more (i) processing operations originally performed for different purposes and (ii) data companies (with at least one being part of the Company) in a way that goes beyond the reasonable expectations of the individual. Examples include combining data collected through cookies with information from job applications, or matching data from different sources.

e) **Processing of sensitive Personal Data**

Sensitive Personal Data may include financial information, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used to identify an individual, data concerning health or data concerning a person's sex life or sexual orientation. Examples include the processing of pictures for skin analysis, information needed to address an associate's disability or criminal records checks for job applicants.

f) **Processing of Personal Data on a large scale**

To determine whether a Supplier is processing a large volume of Personal Data the following factors could be taken into account: (i) The number of individuals concerned - either as a specific number or as a proportion of the relevant population (for example, Personal Data of all the employees of the Company receiving Suppliers' services); (ii) the volume of Personal Data and/or the range of different categories of Personal Data being processed; (iii) the duration, or permanence, of the services entailing the processing of Personal Data; (iv) The geographical extent of the services provided.

g) **Processing of vulnerable individuals' Personal Data**

An individual will be considered 'vulnerable' if their relationship with the Company is one where there is a significant imbalance of control or understanding of the relationship. Examples include children, the elderly, and it is also likely to include employees.

h) **Use of new technology in the provision of services**

For example, technologies such as fingerprints or facial recognition scanners, when they were first introduced to the market for security purposes. It is important to remember that over time, new technologies can become standard practice. One way to consider the distinction is to assess whether the Company's use would be deemed use by a 'first' or 'early' adopter in using it.

i) **Services result in individuals being prevented from exercising a right, using a service, or entering a contract**

This might include processing which screens job applicants based on their qualifications, rejecting certain candidates who do not meet specific criteria, or analysing employee performance based on the number of hours logged, which then determines their annual holiday entitlement.

j) **Using any cookies or similar tracking technologies**

This might include suppliers who use cookies, pixels, tags, device fingerprinting, or similar tracking tools on websites, portals, or applications they operate on our behalf. For example, a supplier hosting a customer-facing portal that uses analytics cookies to track visitor behaviour, or a marketing platform placing retargeting pixels on our web pages to serve personalised advertising.

4. Do you warrant that you have:

a) Process in place to support the DS Smith in fulfilling any data subject rights requests (e.g. access, deletion, correction, opt-outs) within statutory timelines?

Yes No

b) Documented breach notification process that ensures timely notification to clients?

Yes No

5. In the last two (2) years, have you experienced:

a) any security incident/breach(s) that resulted in a notification to a data protection authority/affected individual

or

b) any security incident/breach(s) that results in data protection authority's request/investigation enforcement proceedings.

Yes No

6. Do you have a documented breach notification process that ensures timely notification to clients?

Yes No

7. In the last two (2) years, have you been subject to any data protection authority's request/investigation enforcement proceedings?

Yes No

III. Notification of Changes in Personal Data Processing

The Supplier shall promptly inform the Buyer in writing, without undue delay and in any event within the timeframe specified in the applicable Data Processing Agreement, of any actual or reasonably anticipated material change relating to the processing of Personal Data by the Supplier or any sub-processor engaged by the Supplier in connection with the performance of this Agreement.

Such notification obligation shall apply in particular in the following circumstances:

1. When the Supplier or any sub-processor begins processing Personal Data that it previously did not handle, or was not in the initial scope of processing.
2. When the Supplier or any sub-processor materially changes the method, scope, or purpose of Personal Data processing from what was initially agreed upon.

3. When there is a change in the location of Personal Data being processed in, stored in, or accessed from a different country.
4. When there are significant changes in the Supplier's or any sub-processor's operations, such as changes in the ownership, organizational structure or security practices.
5. When the Supplier or any sub-processor introduces or materially changes the use of automated processing, profiling, or artificial intelligence in connection with the processing of Personal Data under this Agreement.

This notification obligation is cumulative with and does not replace or limit any notification obligation under the AI Risk Due Diligence section of this form, the applicable Data Processing Agreement, or any other contractual obligation between the parties.

IV. Signature

Place / Date:

.....

Company and employee name:

.....

.....

Signature

**Examples of Personal Data:*

- Business contact details (e.g. Name, business email address)
- Identification data, including online identifiers (e.g. Name, address, telephone number, usernames, email addresses, social media handles, login details, social security number, tax identification number, vehicle identification number, license plate number, passport number)
- Biographical data (e.g. Date of birth, age, sex, gender, marital status, place of birth, education records)
- Financial information (e.g. Bank account number, credit card number, credit score, income)
- Employment information (e.g. Job title, salary, work history, emergency contacts)
- Images and videos (e.g. Photographs, CCTV footage)
- Location data (e.g. GPS data, data from mobile devices)
- Device information (e.g. IP address, browser type, operating system, device MAC address and online browsing history)
- Online tracking data (e.g. Cookies, tracking pixels, web beacons)
- Behavioral data (e.g. Purchase history, clickstream data)
- Audio recordings (e.g. Voicemails, phone calls recordings)
- Metadata (e.g. Date and time stamps, file properties)
- Social network data (e.g. Posts, likes, shares)
- Ethnicity / racial origin Health / medical information / disability information Biometric / genetic information Criminal record / criminal offences Trade union membership Political opinion, religious or philosophical views Sexual orientation / sex life