First/current publication: September 2023
Version: 1
Document type: Policy
Scope: Global

DONCASTERS

DATA PROTECTION POLICY

Policy Name
Data Protection.
Purpose
We recognise that the correct and lawful treatment of Personal Data will maintain trust and confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.
Objectives
This Data Protection Policy sets out how Doncasters ("we", "our", "us", "the Company") handle the Personal Data of our employees, workers, business contacts and other third parties. This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, or any other Data Subject.
Audience
This Data Protection Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf. Data protection is the responsibility of everyone within Doncasters and this Data Protection Policy sets out what we expect from you when handling Personal Data to enable Doncasters to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all those Related Policies and Privacy Guidelines. Any breach of this Data Protection Policy may result in disciplinary action.
Confidentiality Status
This Data Protection Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Data Protection Officer.
Local Adaption Authorisation
Yes, if more restrictive.

Document Owner
Head of Legal (Europe)
Document Reviewer
Human Resources
Document Approver
General Counsel & Chief Risk Officer

Data Protection Principles

We adhere to the following principles relating to Processing of Personal Data which state that Personal Data must be:

(a) Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

(b) collected only for specified, explicit and legitimate purposes (purpose limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);

(d) accurate and where necessary kept up to date (accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (storage limitation);

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);

(g) not transferred to another country without appropriate safeguards in place (transfer limitation); and

(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subject's rights and requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability). Each of these principles is described in more detail below.

Lawfulness, Fairness and Transparency

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We may only collect, Process and share Personal Data fairly and lawfully and for specified purposes, some of which are set out below:

(a) the Data Subject has given their Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests; or

(e) to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

We must identify and document the legal ground being relied on for each Processing activity and record this in our Record of Processing Activity which sets out the types of data we hold and the purposes for which we use it.

Consent

A Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity will not be sufficient to indicate consent.

A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible.

Transparency (notifying Data Subjects)

Whenever we collect Personal Data directly from a Data Subject, including for HR or employment purposes, we must provide the Data Subject with all the information required including the identity of the Data Protection Officer, and how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must check that the Personal Data was collected by the third party lawfully and on a basis which contemplates our proposed Processing of that Personal Data.

If you are collecting Personal Data from a Data Subject, directly or indirectly, then you must provide the Data Subject with a Privacy Notice.

Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have Consented where necessary.

If you want to use Personal Data for a new or different purpose from that for which it was obtained, we must first contact the Data Protection Officer for advice on how to do this in compliance with both the law and this Data Protection Policy.

Data Minimisation

We may only Process Personal Data when performing job duties require it. We cannot Process Personal Data for any reason which is not necessary.

We must ensure any Personal Data collected is adequate and relevant for the intended purposes for which it is collected.

We must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention guidelines.

Accuracy

We must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

Data Storage

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after an appropriate time, unless a law requires that data to be kept for a minimum time. You must comply with the Company's Data Retention Policy.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

You will ensure Data Subjects are provided with information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Security, Integrity and Confidentiality

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. We are all responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;

(b) Integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and

(c) Availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with relevant standards to protect Personal Data.

Reporting Personal Data Breaches

We have put in place procedures to deal with any suspected or actual Personal Data Breach and will notify the Data Subject or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches (the DPO). You should preserve all evidence relating to the potential Personal Data Breach.

Transfer Limitation

We may only transfer Personal Data across jurisdictions if one of the following conditions applies:

(a) the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

(b) appropriate safe(guards are in place such as binding corporate rules, standard contractual clauses;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for another legally recognised reason including:

1. the performance of a contract between us and the Data Subject;
2. reasons of public interest;
3. to establish, exercise or defend legal claims;
4. to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and
5. in some limited cases, for our legitimate interest.

Data Subjects Rights

A Data Subject has rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about our Processing activities;

(c) request access to their Personal Data that we hold (including receiving a copy of their Personal Data);

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) object to Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of their country of residence;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

We must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to your site HR manager and the Data Protection Officer.

Accountability

We are responsible for, and must be able to demonstrate, compliance with the data protection principles. As part of this we will:

i. appoint a suitably qualified Data Protection Officer (where necessary) and an executive accountable for data privacy;

ii. implement Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

iii. integrate data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines or Privacy Notices; and

iv. train Company Personnel on this Data Protection Policy, Related Policies and Privacy Guidelines, and data protection matters including, for example, a Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches.

Record Keeping

We will keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records will include:

v. clear descriptions of:

1. the Personal Data types;
2. the Data Subject types;
3. the Processing activities;
4. the Processing purposes;
5. the third-party recipients of the Personal Data;
6. the Personal Data storage locations;
7. the Personal Data transfers;
8. the Personal Data's retention period; and
9. the security measures in place.

Training and Audit

All Company Personnel will have adequate guidance and/or training to enable them to comply with data privacy laws.

We will regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

Privacy by Design and Data Protection Impact Assessment (DPIA)

We will assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

vi. The state of the art.

vii. The cost of implementation.

viii. The nature, scope, context and purposes of Processing.

ix. The risks of varying likelihood and severity for rights and freedoms of the Data Subject posed by the Processing.

We will conduct a DPIA when implementing major system or business change programs involving the Processing of Personal Data including:

x. Use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes).

xi. Automated Processing including profiling and ADM.

xii. Large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data.

xiii. Large-scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

xiv. A description of the Processing, its purposes and our legitimate interests if appropriate.

xv. An assessment of the necessity and proportionality of the Processing in relation to its purpose.

xvi. An assessment of the risk to individuals.

xvii. The risk mitigation measures in place and demonstration of compliance.

Sharing Personal Data

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

We may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

We may only share the Personal Data we hold with third parties, such as our service providers, if:

xviii. they have a need to know the information for the purposes of providing the contracted services;

xix. sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

xx. the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;

xxi. the transfer complies with any applicable cross-border transfer restrictions; and

xxii. a fully executed written contract that contains legally approved third-party clauses has been obtained.

Changes to this Data Protection Policy

We keep this Data Protection Policy under regular review.

This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates. Certain countries may have localised variances to this Data Protection Policy which are available on request to your local Data Protection Officer of the Head of Legal for your region.

Definitions

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies to ensure data protection compliance.

Criminal Convictions Data: personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Officer (DPO): a data privacy manager or other voluntary appointment of a DPO or the Company data privacy team with responsibility for data protection compliance.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with data protection laws.

Privacy Guidelines: the Company privacy guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies, available on the intranet.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of:

a) general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or

b) stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal 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 transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Company's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data, available on the intranet.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.