Privacy Notice

Domino is committed to meeting its legal obligations in respect of all uses of personal data

Which companies does this document apply to?

This Privacy Notice ("Notice") concerns the collection and use of personal information by Domino UK Limited, and the Group functions of Domino (e.g. Group HR, Group Finance, Legal, Group IT, Group Marketing, etc). That includes any Group functions which may operate through Domino Printing Sciences plc.

This Notice also concerns the collection and use of personal information by PostJet Systems Limited and Lake Image Systems Limited.

This Notice is applicable to all current and former employees, workers and contractors of any of the companies referred to above and the Group functions.

In this Notice, references to "Domino" are to the companies and Group functions referred to above.

Other subsidiary companies within the Domino Group should adopt their own privacy notice reflecting local practices and procedures, including local regulations and legal requirements.

What is the purpose of this document?

Domino is committed to protecting the privacy and security of your personal information.

This Notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR) and, where it is applicable in relation to the collection, use or any other processing of personal information done by Domino, other national or international regulations and laws applicable in relation to those activities (collectively, "Data Protection Laws").

For the information which Domino collects, uses or otherwise processes, Domino is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required, under Data Protection Laws, to notify you of the information contained in this Notice.

This Notice does not form part of any contract of employment or other contract to provide services. We may update this Notice at any time, but if we do so, we will provide you with an updated copy of this Notice as soon as reasonably practical.

It is important that you read and retain this Notice, together with the Domino Data Protection Policy and any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the Data Protection Laws.

Data Protection Officer

We have appointed a Data Protection Officer (DPO) to oversee compliance with this Notice in relation to Domino. If you have any questions about this Notice or how we handle your personal information, please contact the DPO. The DPO is John-Paul Martin, General Counsel (johnpaul.martin@domino-printing.com or DPO@domino-printing.com).

Data Protection Principles:

We will comply with the Data Protection Laws. The personal information we hold about you must be:

1. used lawfully, fairly and in a transparent way;
2. collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
3. relevant to the purposes we have told you about and limited only to those purposes;
4. accurate and kept up to date;
5. kept only as long as necessary for the purposes we have told you about; and
6. kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection, such as information about a person's health or sexual orientation.

We may collect, store, and use the following categories of personal information about you. In the case of Domino UK Limited, Lake Image Systems Limited and PostJet Systems Limited most, if not all, of the information will be collected, stored and used. In the case of other Domino companies, we will collect, store and use information necessary for the activities of Group functions, and other information will be processed locally by the relevant Domino subsidiary:

- personal contact details such as name, title, addresses, telephone numbers, and personal email addresses;
- date of birth;
- gender;
- marital status and dependants;
- next of kin and emergency contact information;
- National Insurance/Social Security number;
- bank account details, payroll records and tax status information;
- salary, annual leave, pension and benefits information;
- start date and, if different, the date of your continuous employment;
- leaving date and your reason for leaving;
- location of employment or workplace;
- copy of driving licence (where applicable);
- recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process);
- employment records (including job titles, work history, working hours, holidays, training records and professional memberships);
- compensation history;
- performance information;
- disciplinary and grievance information;
- information about your use of our information and communications systems;
- photographs.

<u>In the case of UK companies only:</u>

- results of HMRC (employment status check, details of your interest in and connection with the intermediary through which your services are supplied; and

- CCTV footage (where applicable) and other information obtained through electronic means such as swipe card records.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- information about your race or ethnicity, and sexual orientation;
- information about your health, including any medical condition, health and sickness records, including:

  - where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;

  - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and

  - where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes;
- biometric data;
- information about criminal convictions and offences, where declared by you.

How is your personal information collected?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies (only in the case of contractors) or other background check agencies. We may sometimes collect results of drug and alcohol testing.

We may also collect personal information from the trustees or managers of pension arrangements operated by a group company.

We may collect additional personal information in the course of job-related activities throughout the period of you working for us.

How will we use information about you?

We will only use your personal information when the Data Protection Laws allow us to. Most commonly, we will use your personal information in the following circumstances:

1. where we need to perform the contract we have entered into with you;
2. where we need to comply with a legal obligation; or
3. where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. where we need to protect your interests (or someone else's interests); or
2. where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. The situations in which we will process your personal information are listed below:

- making a decision about your recruitment or appointment;
- determining the terms on which you work for us;
- enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties;
- liaising with the trustees or managers of a pension arrangement operated by a group company, your pension provider and any other provider of employee benefits;
- administering the contract we have entered into with you;
- business management and planning, including accounting and auditing;
- conducting performance reviews, managing performance and determining performance requirements;
- making decisions about salary reviews and compensation;
- assessing qualifications for a particular job or task, including decisions about promotions;
- gathering evidence for possible grievance or disciplinary hearings;

- making decisions about your continued employment or engagement;
- making arrangements for the termination of our working relationship;
- education, training and development requirements;
- dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
- ascertaining your fitness to work;
- managing sickness absence;
- complying with health and safety obligations;
- to prevent fraud;
- to monitor your use of our information and communication systems to ensure compliance with our IT policies;
- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- to conduct data analytics studies to review and better understand employee retention and attrition rates;
- equal opportunities monitoring.

In the case of UK companies only:

- checking you are legally entitled to work in the UK;
- paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs).

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document (Domino Data Protection Policy) and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. in limited circumstances, with your explicit written consent;
2. where we need to carry out our legal obligations or exercise rights in connection with employment; or
3. where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

Our obligations as an employer

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment. On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so.

We will use your particularly sensitive personal information in the following ways:

- we will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws;
- we will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance;
- we will use information about your race or national or ethnic origin, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so or where you declare it to us. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences to comply with Aviation Security requirements.

We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

DATA SHARING

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside of the UK.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might we share your personal information with third parties?

We will share your personal information with third parties where required by law or where it is necessary to administer the working relationship with you.

Which third-party service providers process your personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group.

Some activities of Group functions involve the use of third-party platforms and/or service providers. In the appendices to this Notice we have listed the key instances and more specific information about them and how they are used.

How secure is your information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might we share your personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share your personal information with a regulator or to otherwise comply with the law.

DATA SECURITY

We have put in place measures to protect the security of your information. Details of these measures are available upon request from the DPO or from your local Data Protection Officer as applicable.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality. Details of these measures may be obtained from the DPO.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

DATA RETENTION

How long will we use your information for?

Where we collect and store information, we will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. The examples below reflect principally information which we collect and store in relation to UK companies, but where any of that information is collected in relation to other companies, we will comply with the legal requirements applicable for the relevant country from which the data originates. This should be covered in the relevant local GDPR policy (which will take precedence in relation to the time frames).

File type	How long information will be kept for
Statutory Maternity Pay records, calculations, MATB1 certificates	3 years after the end of the tax year in which the maternity leave took place
Wages/salary records/overtime/bonus/commission payments	6 years
Records relating to working time or change of working time	2 years from the date on which they were made
Parental leave	5 years from the birth/adoption of the child or 18 years if the child receives a disability allowance
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy

Personnel files and training records	6 years after employment ceases
Redundancy details, calculations of payment	6 years from the date of redundancy
Statutory sick pay records	6 years after the employment ceases
Occupational health records	40 years from the date of the last entry

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention process and Data Protection Laws.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it;
- request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected;
- request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below);
- object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation

which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes;

- request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it;
- request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the DPO in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO.

Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

CHANGES TO THIS NOTICE

We reserve the right to update this Notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this Notice, please contact John-Paul Martin, General Counsel at johnpaul.martin@domino-printing.com.

APPENDIX I - CONNECT

Data access in Connect

System access

All users have a Domino email account set up by Group IT and their credentials are validated when logging in by the Domino Active Directory server including 2 Factor Authentication (2FA).

System records (back end)

- All employee records in Connect are segregated by **HR department**
- All access to employee records is controlled by **user profile:**
    - Default profile is **Team Member** with no access to any employee records
    - **HR manager** only has access to records in the HR department they have been assigned to. The HR manager role is assigned to local HR managers and administrators.
    - **HR administrator –** access to all records across all HR departments, assigned to a limited number of people in Group HR and Group Finance
    - **System administrator –** access to all records and config, assigned only to HRIS administrators

WX (Connect web portal) access

- Each employee has access to view and update their own personal information and view their own contract details including salary.
- Line managers can view contract details including salary, absence information (in relevant territories) and objectives/performance reviews and talent plans and recognition (everywhere except Germany) for their reports; they can also run reports, restricted to the above data, for their teams (employees in their reporting line)

Scheduled reports and integrations

Domino Academy automatically synchronises active users but only uses their name and email address and employment status.

Some system data reports are sent to Group IT and Group Finance for validation against other systems and to update other data (e.g. to synchronise with Microsoft Active Directory). These are password protected.

Auditing

- Changes to data in key fields in each object are recorded
- Login information for all system users is recorded for each session

APPENDIX 2 – MS Productivity

Data access in *Microsoft Productivity (MyAnalytics)*

Domino uses the same Microsoft Tenant for all Domino locations, which means it is one setting for all. Currently there is one configuration setting "allow data to be used for people experiences scoring" and currently this configuration setting is set as "not allowed".

System access

All users have a Domino email account set up by Group IT and their credentials are validated when logging in by the Domino Active Directory server including 2 Factor Authentication.

Purpose

MyAnalytics can help participants strengthen their work relationships, have more time to focus on important work, and improve their work-life balance. *MyAnalytics* does this by showing users insights about their work habits. It derives these insights from *Microsoft 365* data about emails, meetings, calls, and chats.

Insights - what kind of insights does the employer actually get and which kind of employees' personal data are involved?

The *MyAnalytics* dashboard opens to the Home page that shows you statistics about your work patterns over the past month, including your focus and collaboration time, how many days you were able to disconnect from work, and how effectively you are networking with your co-workers.

MyAnalytics Insights emails are private to the individual.

Unlike productivity apps that encourage sharing and collaboration, *MyAnalytics* is meant to be private user information. The information it pulls from your email and calendar can only be viewed by the user.

Domino does not get the detailed information as to how busy people are, it is more about the statistics as to how many meetings they attended, etc. For more information see – *https://docs.microsoft.com/en-us/microsoft-365/admin/productivity/productivity-score?view=o365-worldwide*

I have heard that Microsoft had to make changes to *Productivity* to deal with Data Protection issues. What were those ad where can I find out about Microsoft's commitments to privacy?

Please see the Microsoft Blog post at this address for more information on this:

https://www.microsoft.com/en-us/microsoft-365/blog/2020/12/01/our-commitment-to-privacy-in-microsoft-productivity-score/

What access do Group IT have to information generated through or by *Microsoft Productivity*?

There are 3 people in Group IT that have access to the configuration of MS Productivity. In the Category details section of this link, it shows the primary insight and supporting metrics available to an Admin. https://docs.microsoft.com/en-us/microsoft-365/admin/productivity/productivity-score?view=o365-worldwide

What commitments do Microsoft make about their processing of personal information, including any personal information involved in *Microsoft Productivity*?

Please see more about Microsoft's commitment in respect Generally Available Enterprise Software Products at *https://docs.microsoft.com/en-gb/legal/gdpr*. Also Microsoft's General Data Protection Regulation (GDPR) page at: *https://www.microsoft.com/en-us/professionalservices/gdpr*.