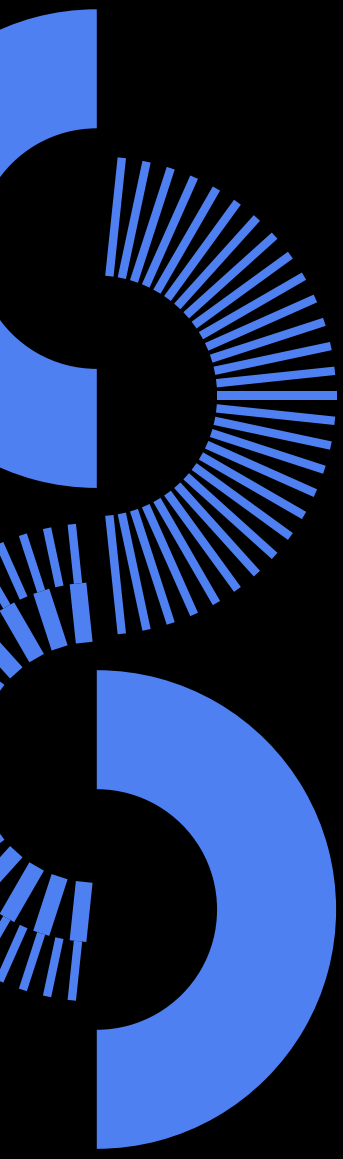
OMNICOM

GLOBAL DATA PROTECTION & PRIVACY POLICY

UPDATED NOV. 2025

CONFIDENTIAL —
NOT FOR EXTERNAL
DISTRIBUTION



Document Controls

Table 1: Governance Information and Policy Management

Document Name	Global Data Protection and Privacy Policy	
Document Type	Policy	
Document Classification	Confidential	
Document Owner	***Legal & Privacy***	
Geographic Application	Applicable Worldwide (subject to laws in each jurisdiction) The document covers all of Omnicom Group and its agencies.	
Reviewed by	Omnicom Information Risk Management Committee	
Approved by	Omnicom's Information Risk Management Committee has reviewed this policy and hereby sign it into effect.	
	Robert H. Cohen **Senior Vice President, Deputy General Counsel - Litigation & Employment Member, Information Risk Management Committee**	Robert Cohen
	Brian F. Clayton **Associate General Counsel and Chief Data Privacy Officer**	Brian Clayton
	Craig Cuyar ***SVP and Global Chief Information Officer***	Craig Cuyar (Oct 9, 2025 10:07:12 EDT)
	Paul Scott ***Global Chief Information Security Officer***	
Issued Date	2025-10	
Last Reviewed Date	2025-09	

Table 2: Version History

Version	Date Signed	Issued Date	Description of Input or Changes
1.0	December, 2021	January, 2022	First Release
1.1	June, 2023	July 1, 2023	Administrative updates 2023
1.1	Oct, 2024	Oct, 2024	Annual review- No changes made
2.0	August, 2025	August, 2025	Updates to section 2.11 Data Retention
2.1	October, 2025	October, 2025	Minor changes to correct typo in the footer

This Global Data Protection and Privacy Policy is one of Omnicom's Information Security 'Topic' Policies. These are governed by Omnicom's 'Core Information Security Policy'. The terms and requirements of the Core Information Security Policy apply to this Policy.

Unless specified otherwise:

All references to Omnicom's 'Information Security Policy' should be taken to include both the Core Information Security Policy and all Information Security Topic Policies; and

A reference to the Core Information Security Policy refers to that document specifically.

All Omnicom security policies currently in force (inc. the Core Information Security Policy and other Information Security Topic Policies) can be found at: https://oneomnicom.sharepoint.com/sites/OMC-ITCentral

All Omnicom policies are originated in English. Translations may be provided in local language for convenience, but in the event of any conflict/interpretative differences, the English version will always take priority.

Contents

PART 1 – Introduction

In its everyday business operations, Omnicom, its Networks, Practice Areas and Agencies make use of a variety of personal data, including:

- Data about current, past and prospective employees and consultants;
- Data about current, past and prospective clients;
- Data about current, past and prospective third-party visitors (e.g., auditors, partners, and other visitors);
- Data we process *on behalf* of clients, or as part of our services, including that relating to journalists, bloggers, talent, social media influencers, client contacts, market research participants, industry contacts, or other stakeholders relevant to the work we do; and
- Data about users that is collected from our websites.

Omnicom and Agency data may be held by us directly, or supplied, maintained or administered internally by third-party suppliers/vendors. The data can be held on our IT systems, electronic devices or on hard copy documents.

This Global Data Protection and Privacy Policy (the "Policy") establishes the principles, procedures and best practices for protecting and safely handling Omnicom and Agency data. It describes the role and responsibilities of Omnicom and Agency personnel in assuring that personal data is always kept safe and secure. Further, it sets out the ways in which we must comply with data privacy laws across our businesses.

1.1 Audience and Scope

This Policy applies to anyone performing services for or on behalf of Omnicom Group, its Networks, Practice Areas, Agencies, Affiliates, Associations, and Subsidiaries. This includes all employees, officers, volunteers, interns, casual workers or agency workers retained by any of the above, plus any consultants, contractors or freelancers (whether retained directly or using a personal services company). Therefore, when we use the terms 'employee' or 'employment' or 'staff', we mean all these categories of workers.

We operate across the globe and so this Policy is intended to address multiple jurisdictions' privacy laws and requirements including those of the GDPR, CPRA/CCPA and HIPAA/HITECH (the "Data Privacy Laws"). Because of this geographic scope, this Policy cannot be completely comprehensive because it is possible that, in some circumstances, local Data Privacy Laws, regulations or government guidance may conflict with the provisions of this Policy. In the event of such conflicts, the Data Privacy Laws should prevail over this Policy.

Networks, Practice Areas and Agencies may also put in place their own data protection policies to supplement the requirements of this Policy.

1.2 Where do you come in?

This Policy applies to you if you have access to Omnicom and Agency data and/or IT systems which allow access to it. Additionally, it applies to you if you have access to client personal data. If this Policy applies to you, you must read and comply with it.

Compliance with Data Privacy Laws requires Omnicom's employees and business partners' commitment, participation, and accountability. Therefore, employees must follow this Policy and all other policies governing our approach to information security and data protection.

These policies can be found here:
Security Policies (sharepoint.com)

or

https://www.omnicomgroup.com/culture/ethics-policies/

1.3 Key Definitions

In this Policy, the following terms have the following meanings:

- **"consent"** means that the data subject freely agrees (by an affirmative act) to the processing of his or her personal data. The information must be given to the data subject in a clear and unambiguous manner.
- **"data controller"** means the organization that determines the purposes and means of processing personal data.
- **"data subjects"** are the natural persons to whom the personal data relates.
- **"data processor"** means an organization that processes personal data on behalf of a data controller.
- "**personal data**" under the GDPR means any information relating to an identified or identifiable natural person. An identifiable natural person is someone who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It includes not only facts about an individual, but also intentions and opinions about an individual. Examples of personal data range from IP addresses to performance evaluations.
- Privacy legislation outside the UK/EU may have a slightly different definition; in some cases, the definition may be narrower than what is described herein. However, for the purposes of this Policy, we have chosen to apply the wider GDPR definition. As such, unless specified, when we talk about "personal data" we are also talking about broadly analogous concepts under local laws including "personal information" and "PII".
- **"Personal Information"** means any information or collection of information that pertains to an individual; it can be in any form, e.g., oral, electronic or written. Excluding:
    - Information that is publicly available
    - Information that is used for business communication such as: title, business address, business email and business telephone

  When we talk about "personal *information*" (as opposed to personal *data*) we are referring to this definition specifically.

- **Personal identifiable information (PII)** means any information about a person including but not limited to:
  - Information used to distinguish or trace the individual's identity such as:
    - Name;
    - An identification number, e.g. social security number;
    - Date and place of birth;
    - Mother's maiden name;
    - Biometric records.
  - Other information that is linked or linkable to an individual such as:
    - Medical;
    - Educational;
    - Financial.

  When we talk about PII (as opposed to personal data) we are referring to this definition specifically.

- **"GDPR"** means the General Data Protection Regulation (EU) 2016/697, which applies in the EU. However, for the purposes of this Policy when we say "GDPR" we also mean the UK GDPR, a version of the regulation which applies in the UK post-Brexit.
- "**processing**" means doing anything with the personal data. For example, it includes collecting it, holding it, disclosing it and deleting it.
- **"special personal data"** is personal data that reveals racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, data concerning health or a person's sex life or sexual orientation, biometric or genetic data and personal data relating to criminal convictions and offences.
- **"supervisory authority"** means the regulator or body responsible for data privacy compliance in the jurisdiction in question.

1.4 Wording Conventions

Policies and standards requirements are identified as follows:

- Shall/will/must: a mandatory requirement
- Should: a guideline or recommendation that is strongly encouraged
- May: an action that you are allowed to do

1.5 Policy compliance

Breach or a suspected breach of this Policy may lead to us revoking your access to our systems. It may also result in disciplinary action up to and including the termination of your engagement with us. Where appropriate, performance improvement processes may also be undertaken. Such action may be taken whether the breach takes place at your normal place of work or not and whether the breach is committed outside office hours or not. You will be required to co-operate with any investigation into a suspected breach; this may involve providing us with access to any relevant device and access credentials.

Please note, if you are not an authorized user or if you lose authorization to access Omnicom's systems and data, you are prohibited from accessing or attempting to access such data. Unauthorized access may be subject to criminal prosecution.

1.6 Accountability and Privacy Roles

Data Protection Officers (DPOs) and/or Data Privacy Leads (DPLs) within each Agency or Practice Area have the overall responsibility for the day-to-day implementation of this Policy and related non-compliance matters. For information on changes to this Policy – see Part 3.

The DPO role is a dedicated position and shall be filled by at least one person in each Network or Practice Area and at the Omnicom level. Some regional regulatory requirements may mean that some Networks, Practice Areas and Agencies also have regional DPOs. The DPO role has been aligned with the GDPR role requirements but in essence, the DPO independently ensures that their organization applies the laws protecting individuals' personal data, including:

- informing and advising employees about their obligations;
- monitoring compliance with the GDPR and other data privacy laws, as well as with Omnicom and Agency data protection policies;
- advising on and monitoring data protection impact assessments;
- raising awareness of data protection issues;
- training and mentoring staff on data privacy and data protection matters; and
- liaising with and being a point of contact for both data subjects and supervisory authorities.

Some of the DPO's responsibilities (and privacy expertise in general where a DPO is not legally required) may be delegated to individuals that have proficiency with privacy, (e.g. an attorney, privacy manager, data champion, data protection lead, etc.) each a **Data Privacy Lead ("DPL")**. The DPL role is typically performed at an Agency or Practice Area level; every Agency is required to either appoint a DPL or have reasonable and timely access to a DPL at the Practice Area level commensurate with the Agency's complexity. This role can be taken on in addition to other responsibilities, although in some cases, the DPL role may be dedicated because of the size of an Agency or Agency group. The DPO and/or DPL shall advise their organization about data protection matters, maintain a record of processing activities, ensure that privacy training is attended and (in connection with legal counsel and/or the Chief Data Privacy Officer) coordinate with supervisory authorities .

Data Owners, also referred to as Information Owners, are either individuals or teams who make decisions about the data e.g. who can access the data, who can edit it and how should the data be used and/or classified. Although data owners do not necessarily work with their data every day, they are nonetheless responsible for overseeing and detailing what is required to protect the data domain. The data owner will also be responsible for determining and logging what privacy regulations apply to data sources where appropriate. Data owners are also in charge of granting permissions to access the data in question.

Data Custodians, also referred to as Information Custodians, are responsible for managing the information systems as required by applicable corporate policies and data owner instructions. Data custodians are responsible for implementing and enforcing controls that ensure the confidentiality, integrity, and availability of the information housed on the various platforms they manage.

A **Data Source, also referred to as Information Source,** is defined as a data repository that can be structured, semi-structured **or** unstructured.

1.7 Contact Information

If you have any questions about how to handle a data privacy matter within your Agency or Practice Area, please contact the appropriate DPO and/or DPL. If you are unsure who to reach out to, please e-mail privacy@omnicomgroup.com and someone will point you in the right direction.

PART 2 - Data Privacy Policy

2.1 General Principals

The OMC Privacy Program's requirements are tailored to the European General Data Protection Regulation (GDPR) because it is the most stringent regulation that has been enacted in law to date. Not only is this a best practice but adopting GDPR as a foundational principle also enables the organization to implement high standards for complying with data protection rules while maintaining a consistent approach for handling personal data globally. As such, our guiding principles with respect to how personal data should be handled is as follows:

- Processed in a fair, lawful and transparent manner;
- Collected only for specified, explicit and legitimate purposes;
- Limited to processing only what is necessary (for the intended purpose);
- Retained only for the length of time required to process it (and for the originally intended purpose);
- Kept as accurate and up-to-date as possible;
- Processed in a manner that ensures its security using the appropriate technical and organizational measures to protect against unlawful or unauthorized processing, accidental loss, destruction or damage;
- Transferred to other countries with the appropriate safeguards; and
- Upon request, made available to data subjects should they want to exercise their right to learn what information is recorded about them and how we use their information.

However, bear in mind that local or regional laws may take precedence where they differ from GDPR. This is because Omnicom and its Agencies comply with all privacy laws and regulations that are relevant to the locations in which we operate. Therefore, you are required to treat personal data in a manner that is consistent with local or regional laws and regulations.

2.2 Our role and the type of personal data we collect

Omnicom and its Agencies engage in different data processing activities e.g. data processing to fulfill contractual relationships, to satisfy legal obligations or to conduct consent-based processing from our consumers. In some circumstances, we play the role of a controller while in others, we serve as a processor (see above for definitions).

We act as a **controller** when we process the personal data of our employees, customers or when we dictate to a third party how the processing of such data should be handled. For example, this would include:

- **Data about our customers/clients**: personal data about our clients / customers may be collected directly from e.g. consent forms on our websites, or indirectly via automated means

e.g. cookies, web server logs, web beacons and other technologies. It may also be sent to us via email or created as part of the work we do.

- **Employee data**: the personal data of an employee is collected from the moment they apply for a position. Omnicom and its Agencies collect and store this information in order to support employees during the course of their career. Further, we are required to keep the personal data of employees to comply with tax and employment laws.

- **Other third party data:** for example, we will process personal data about vendors, business partners, visitors, as well as (in some cases) consumers, media and industry contacts, and other stakeholders.

When we process data *on behalf* of our clients, we are serving as **processors**. The personal data that we collect and process on behalf of our clients should be specified in the contract we sign with them (see section 2.6 for more on what to do when sharing or receiving data from clients). For example, the contract will indicate what type of data we should process and what should happen to it once the contract is terminated. When we process data regarding third parties (including consumers, media and industry contacts, social media influencers and other client stakeholders) for a client, it may be that we are doing this as processor for them.

2.3 Data Processing

Legal Basis

We cannot collect, process or sell any personal data unless we have a valid, legal justification for doing so. We are obligated under law to be able to justify our actions using at least one[1] of the following reasons:

- **Consent**: data subject(s) has explicitly opted in;
- **Contractual**: processing is necessary to execute a contract that the data subject(s) is involved in;
- **Legal obligation**: processing is necessary to comply with a legal obligation to which we are subject; or
- **Legitimate interest**: there is a compelling business reason that doesn't take away from individual rights and freedoms.

Records of Processing

Irrespective of our role in the data lifecycle, Omnicom and Agencies must keep records of processing activities ("ROPAs" or "Article 30 Records") in order to demonstrate compliance to supervisory authorities. The processing records shall contain information such as a description of the categories of data subjects and the types of personal data, the purpose(s) of the processing, the legal basis for each processing activity and information regarding the transfer of data to third parties.

Refer to the Records of Processing Guide to see the list of data elements that should be captured in a ROPA for controllers and processors.

[1] Additional reasons that could be used to justify processing were excluded because they don't apply to our areas of business; they are:

- Life threatening: to save a life
- Public interest: to carry out an official government or related task

Omnicom Group's ROPAs shall be maintained in the Privacy Information Management System (PIMS).

DPOs or DPLs are responsible for maintaining and editing ROPAs; individuals in these roles shall ensure that the processing records of their Agency or Practice Area meet OMC standards in terms of data quality.

Individuals who are involved in data processing activities, including data owners, shall follow the instructions given by the DPO or DPL if they find that their data processing activities require modification (typically to better meet legal obligations or to strengthen standards). On the other hand, data owners shall inform their DPO or DPL when an update is necessary to processing records, e.g. when their agency engages a new data processor to process personal data. Data owners should not update ROPAs without input from a DPO or DPL.

ROPAs shall be reviewed:

- when/if events occur that require a review and a possible update e.g.:
  - data breach
  - implementation of a new system
  - decision to broaden the scope of the business
  - decision to change the purpose for which the data is processed;
- or at a minimum, annually.

Further, all data sources that are known to store or believed to store PII, PHI, intellectual property data, and any other data classified as either confidential or restricted per the definitions above, should be onboarded to the Omnicom Data Governance as a Service (DGaaS) platform for recurring scanning to maintain an accurate and up-to-date catalogue and inventory of data elements as defined by recognized regulatory bodies (e.g. GDPR, CCPA/CPRA, PCI, HIPAA, etc.). Data Sources storing data classified as internal may be onboarded to the DGaaS platform at the discretion of Omnicom IT and the owning Network, Practice Area or Agency.

Purpose Limitation

You must not access, modify or process any personal or confidential information that belongs to Omnicom, its Networks, Practice Areas, Agencies, employees, partners vendors or clients without a proper purpose and legal basis (see above); nor may you share or transfer such data to any party that does not have a legitimate business need for it (please see section 2.6, Data Sharing for more details).

For example, if you receive information for a vacancy from a prospective employee, you should only use that information for the specific job applied to. The information received should not be reused for a different job unless the applicant was informed that we may hold their information on file for consideration of other vacancies. Ask your DPO/DPL when in doubt about how to handle personal data.

Responsibility of Employees (including consultants, contractors, interns)

As an employee, consultant, freelancer or intern, you shall comply with the following:

- Only share personal data with colleagues who are authorized to use it;
- Maintain the security of the personal data that you use or are responsible for, e.g. by using complex passwords and locking your computer when you leave it unattended;
- If you develop software, you are required to use privacy by design and privacy by default principals, see section 2.9 for more information;

- If you are involved in the procurement of IT systems/services where personal data will be processed:
  - Include requirements on the system/service that will make it possible to restrict access, protect and erase personal data;
  - Ensure that you are informed of any sub-contractor that will process the personal data.

If you are procuring cloud services, be mindful of the location of data processing as that will impact which privacy regulations will be triggered.

As an employee, consultant, freelancer or intern, you shall comply with the following instructions when you process personal data in your employment with or assignment for us:

- Ensure that personal data processing agreements and data transfer agreements are in place with service providers before engaging with them to transfer personal data. If you are unsure, confirm with your manager or the sponsor of your contract, or e-mail privacy@omnicomgroup.com;
- Ensure that there is a legal basis to process personal data in the way you intend to process it; if in doubt, confirm with your DPO or DPL:
  - Keep in mind the principles that are outlined in section 2.1 and the definition of processing;
  - Limit the collection and processing of personal data; do not collect personal data that is "nice to have"; collect and process only what you "need to have" for a specific purpose (it should align with one of the justifiable reasons listed above);
  - Do not use national identification numbers, e.g., social security numbers, unless there is a strong business need for them e.g. for tax identification purposes;
  - Limit the processing of special categories of personal data such as health and ethnic origin.
- Ensure that the personal data that you process is accurate and up to date;
- Erase personal data that you have stored on your computer if it is no longer needed; consider the retention policy and the purpose for which the data was originally collected.

Regardless of your role, remember that your email account and your work computer are company property and should be used as necessary for work related purposes. To a limited extent and within reason, they may be used for private purposes. However, if you use them for personal reasons, keep in mind that your Agency will treat the data that is stored on them as information that belongs to it (please see the Acceptable Use Policy for more information).

2.4 Transparency

Transparent communication to data subjects about how their data is processed is integral to data privacy laws. OMC has put in place privacy notices to meet these requirements; one such notice is a workplace privacy notice that outlines how we process employee data.

Practice Areas and Agencies will need to have similar employee notices as well as notices that cover the processing of third-party data (including clients, consumers, vendors and website users - an “External Notice”). We created an External Privacy Notice template to assist our Practice Areas and Agencies; it should be modified to suit the specific needs of the Practice Areas or Agency in question.

2.5 Security

Data privacy laws require that we keep personal data secure by putting the appropriate technical and organizational measures in place. The following policies were created with these requirements in mind:

- Omnicom User Information Security Manual (and any other policies relating to IT or information security processes)
- Omnicom Acceptable Use Policy
- Omnicom Bring your own device ("BYOD") Policy
- Data Classification Policy

Data Classification, also referred to as Information Classification

We also implemented a Data Classification Policy that contains specific rules on the storage, transfer, access to and disposal of different types of information (including but not limited to personal data).

Data Breaches and Security Incidents

If a data breach occurs, we must take swift action to respond to and control the breach, and in some cases, notify the relevant supervisory authority and data subjects. We need your help in doing this.

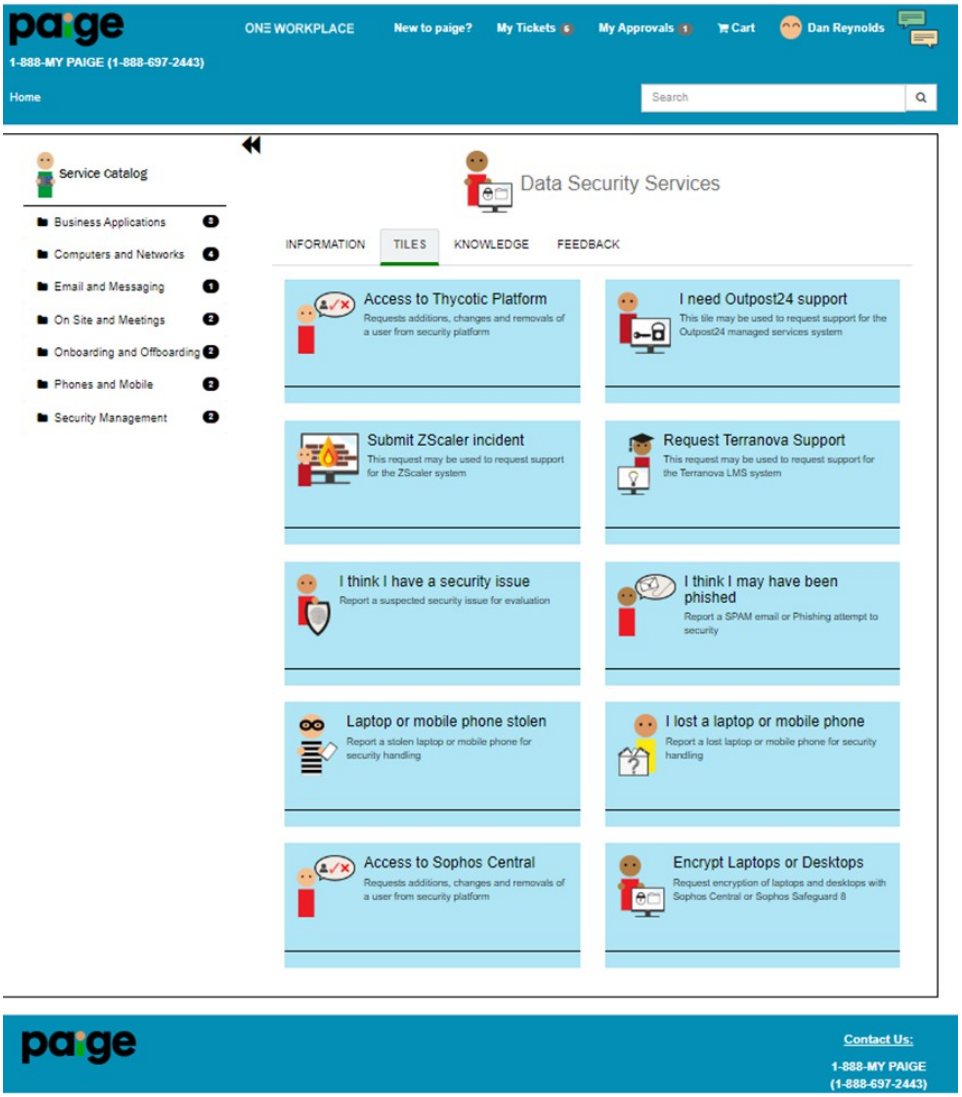
A **"data breach"** occurs where there is destruction, loss, alteration or unauthorized disclosure of or access to personal data that is held, stored, transmitted or processed. For example, if you lose a laptop or a USB stick or if you send an email to the wrong person by mistake, a data breach could occur if personal data was involved in that action.

A **"security incident"** refers to any event resulting in a breach of security or unauthorized access to or acquisition, release, use or disclosure of information on our systems (even if this does not include personal data). Data breaches will typically also be security incidents, but security incidents can occur without involving personal data; examples of the latter include:

- strange or abnormal activity such as pop-ups on your workstation or laptop; or
- any suspected or known unauthorized disclosure or use of confidential *corporate* information.

In either case, if you suspect there has been a data breach or security incident this **must** be reported **immediately** to Omnicom Security Services via the following methods:

- email to SOC@omnicomsecurityservices.com; or
- completion of the appropriate service tile on the Paige service portal as shown below.



You must also notify your Business Information Security Officer (BISO) and Data Protection Officer (DPO) or Data Privacy Lead (DPL). The contact details for your BISO and DPO/DPL can be found in the Helpful Resources document.

If you are a contractor or vendor, you may not have access to the above tile, in such cases reach out to your main point of contact at Omnicom or to the sponsor of your contract so that they may report the incident in ServiceNow.
The exposure of data is important to us as an organization. So, if for example, you lose your work computer or accidently leave it on a train, report it without delay. Time is of the essence because we may need to report the data loss to a supervisory authority (sometimes within 72 hours). As such, failure to notify a security/data breach or to provide follow up information related to a breach will be treated seriously and may lead to disciplinary action.

If it is confirmed that a data breach occurred, the risks involved will be assessed and the regulatory and/or contractual obligations that apply will evaluated. Then a decision will be made on whether or not the breach could risk the rights and freedoms of the affected data subjects and whether it is necessary to notify them. The assessment and associated decisions will be made under the direction of legal counsel.

Additionally, if it is confirmed that a data breach occurred, the incident shall be recorded in the Data Breach Log by the DPO or DPL. The Data Breach Log shall include relevant facts such as:

- The event(s) that took place;
- The data that was affected and its scope;
- The consequences and actions that were taken; and
- The decisions that were made and the reasons why they were made.

The Data Breach Log shall be used as a mechanism for confirming compliance with regulatory laws upon request. Incidents in the Data Breach Log shall not be modified after completion. The Data Breach Log is subject to confidentiality; it shall be maintained by DPOs and DPLs. Breach notification templates shall be created and updated by OMC Legal.

2.6 Data sharing

All employees must think carefully before sending data to third party organizations. In particular, you should not send personal data to third parties unless you know that they are authorized to receive it and that the data is being shared for a valid purpose. Again, ask your DPO/DPL when in doubt about how to handle personal data.

Further, you may not publish personal data belonging to Omnicom or its Agencies to external sites without authorization. In particular, you must not publish confidential client or employee information to any social media site including but not limited to: Twitter, Facebook, LinkedIn, Google+ and YouTube without authorization.

We have set out below some further information about common sharing scenarios.

Third party service providers
Omnicom and Agencies have contracts with service providers who process personal data on their behalf e.g., payroll agencies and cloud service providers. When we contract with data processors, we are required to impose terms on them that limit how the data can be used; we can also impose obligations related to the confidentiality, security and inspection of that data.

Data sharing and processing agreement templates were created as part of our privacy compliance strategy. These templates are intended to be used as a guide when drafting or reviewing data processing/sharing terms. There is also Guidance Note on how to use them. However, it is strongly advised that you seek legal support when dealing with such agreements.

Before onboarding a new processor, you should also ensure that sufficient due diligence has been carried out in relation to the technical and organizational measures used by the processor. In practice, this means that **any new third party processor must be approved by Omnicom via successfully passing the Omnicom vendor risk assessment** (with no open risks that are not covered by an approved risk exception). To learn more about the Vendor Risk Assessment process, please visit: https://oneomnicom.sharepoint.com/sites/OMC-ITCentral/SitePages/Vendor-Assessment.aspx

Clients
We often share personal data with our clients or process personal data on behalf our clients, so in most cases we will need to have the appropriate data privacy terms in place to cover the processing and/or sharing of such information. The data processing / sharing agreements referred to above also contain versions that are suitable for contracting with clients (they may be used as a guide if reviewing terms drafted by the client). Again, it is advised that you involve someone from your legal team to oversee this process.

2.7 Transferring data outside the UK/ EEA

To the extent that Omnicom and/or any Agencies are caught by the requirements of the GDPR (as well as UK GDPR and/or Swiss Data Protection laws) personal data must not be transferred to a territory outside of the UK/EEA/Switzerland ("Restricted Territory") **unless** an exemption applies **or** the appropriate safeguards are in place (the "International Transfer Requirements").
Exemptions Omnicom and/or an Agency might be able to rely on if they wish to transfer personal data to a Restricted Territory include:

- the European commission or UK Government (as appropriate) has issued an "adequacy decision" in respect of the jurisdiction in question[2];
- the data subject has explicitly consented to the proposed transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller; or
- the transfer is necessary for the establishment, exercise or defence of legal claims**.**

If Omnicom and/or an Agency is unable to rely on an exemption, a commonly used safeguard is to put in place a set of terms drafted by the EU Commission (called the "Standard Contractual Clauses" or "SCCs") between the entities exporting and importing the personal data. If you intend

to use SCCs to transfer personal data to a Restricted Territory you should ensure an appropriate risk assessment is carried out – see further below for details.

Please note, the US Privacy Shield used to be considered an appropriate safeguard but has now been invalidated by EU case law and can no longer be relied on for this purpose.

Internal Transfers using the SCCs – further information
To cover the sharing of personal data between Omnicom and our Principal Agencies, we have put in place Intra Group Data Sharing Agreements ("IGDSAs") that incorporate the Standard Contractual Clauses. These IGDSAs provide a safeguard for transfers between Omnicom and Principal Agencies. Please contact your DPO to obtain more information about IGDSAs.

Agencies should ensure they have similar arrangements in place to cover transfers within that Agency's group (for example where a UK/EU Agency entity transfers data to an Agency entity based in the US). We have provided a template IGDSA that can be used for this purpose. For further information about these IGDSAs please contact your DPO.

External Transfers using the SCCs – further information
If data is being transferred to a third party in a Restricted Territory (for example to a vendor or to a client) **and** an exemption does not apply, we will need to ensure there is an appropriate safeguard in place to cover the transfer to the third party. This will likely mean that you will need to ensure that the Standard Contractual Clauses are incorporated into the data processing/sharing terms that were concluded with the third party. The template data sharing/processing agreements for clients and vendors mentioned above include versions that incorporate SCCs.

---

[2] *As of November 2021 - decisions have been issued in respect of: Andorra, Argentina, Canada (commercial organizations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, the United Kingdom and Uruguay. For further information see here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Transfer Impact Assessments ("TIAs")
Where Agencies and/or Omnicom rely on the SCCs to lawfully transfer personal data to a third party in a restricted territory, they also need to carry out a TIA. A TIA is a form of risk assessment that considers the legal system (and in particular surveillance laws) of the jurisdiction in question to assess whether, taking into account any further measures put in place by the parties, the SCCs can offer sufficient protection to data subjects in practice.

TIAs have been carried out in relation to the sharing of data between Omnicom and Principal Agencies. However, where Agencies (a) use the template IGDSA to share data within that Agency group, or (b) use the template data sharing/processing agreements with external third parties as mentioned above, they will need to carry out their own TIAs before sending data. For more information about conducting a TIA, please speak to your DPO.

2.8 Data Subject Rights Requests

Under the GDPR, individuals have several rights (which may be exercised via a "Request"). These rights are:

- the right to access their personal data;
- the right to correct their personal data;
- the right to erasure of their personal data;
- the right to portability of their personal data from one data controller to a new data controller;
- the right to restrict processing of their personal data; and
- the right to object to the processing of their personal data.

Further detail about the GDPR rights is set out in Schedule 1.

Other data privacy laws give similar rights to data subjects, for example the California Privacy Act ("CCPA") has a similar right to access. However, the remainder of this section focuses primarily on GDPR rights.

What to do if you receive a Request?
If you receive a Request from an individual, such a Request should immediately be forwarded to your DPO. It should be agreed with the DPO who will lead on responding to the Request and the steps outlined below. Sometimes these steps may be carried out by the DPO and sometimes they may be done by a DPL. However, for ease, the remainder of this section just refers to "you" as the person responsible for carrying out this request.

Confirm ID
Upon receipt of a request, you should:

- verify that the scope of the Request is sufficiently clear. If it is not clear, you should contact the requestor to request further information. The types of further information that may be required in respect of each of the rights are set out in Schedule 1; and

- check whether the identity of the requestor has been verified. If a Request is made by an individual other than a current employee, the data controller is only obliged to comply with the Request if the individual making the Request supplies it with information that allows it to confirm their identity. This should comprise **proof of identity** (e.g., copy of passport, driving license or ID card) and **proof of address** (e.g., recent utility bill or bank statement). You should contact the requestor to ask for such information if it has not been provided.

You should acknowledge the Request once you have received additional information required about the scope of the request and appropriate identification documents from the requestor. You should then

determine whether the Request is valid. Information about whether GDPR Requests are valid is set out in Schedule 1.

Actioning the Request
You should follow the appropriate steps for actioning the Request. Relevant considerations with respect to each right are set out in Schedule 1. It is important to keep a record of the steps taken when responding to the Request.

In some cases, actioning a Request may require third parties such as service providers to carry out data processing on our behalf (e.g., to amend their records in response to a request to rectify personal data or to delete personal data they hold in response to a Request for erasure - see Schedule 1 for more details). In other cases, we may also be obliged to inform third parties such as clients or partners with whom we have shared data with about Requests.

Timescales
While actioning requests, bear in mind statutory timescales and whether an extension of time is needed under local laws; for GDPR requests this is normally one month. Contact your DPO or DPL if it is possible that actioning the Request will take longer than the requisite timescale. For GDPR requests, this will normally mean contacting the requestor to inform them that the response to the Request will be delayed and the basis for this extension of time (normally that the Request is complex under Article 12(3) GDPR).

Fees
Please speak to your DPO or DPL about whether you should charge a fee for Requests. However, for GDPR Requests Omnicom and Agencies are not permitted to charge a fee for handling the Request unless the Request is “manifestly unfounded or excessive.”

Refusing a Request

If you are not going to respond to the Request (e.g., because it is invalid) you must discuss this with your DPO or DPL. For GDPR Requests this will mean informing the requestor of the reason(s) for not acting and of the option to lodge a complaint with their local data protection authority.

2.9 Privacy by Design

We must integrate data protection and privacy features into our information systems including the design of networked ecosystems and the application development process. To achieve this, Omnicom and its Agencies shall adopt the seven principals of Privacy by Design (PbD) as listed below:

- Proactive not Reactive/Preventative not Remedial
    - The concept that data privacy shall not be an afterthought is at the heart of the PbD principal; it must be considered at the planning phase in order to set a commitment to high standards of privacy at the inception of an initiative.

- Privacy as the Default
    - Personal data should be automatically protected. No action should be required of individuals in order to protect their information. This means, for example, the default settings on a user interface should be automatically configured to the settings that offer the greatest level of privacy for the end user.

- Privacy Embedded into Design
    - Data privacy should be a considered as a core functionality. Privacy assessments should be conducted when necessary, in order to minimize risks. Also, there should be rigor in minimizing design flaws that lead to data security vulnerabilities.

- Full Functionality – Positive-Sum, not Zero-Sum
    - There shouldn't be a trade-off between privacy and functionality. If done correctly, functionality shouldn't be diminished because of privacy requirements. All requirements and/or business objectives can be pursued and implemented while embedding privacy into the design.

- End-to-End Security– Lifecycle Protection
    - The lifecycle of the data, from the time it is collected to when it is disposed of, must be secure. End-to-end security is crucial because data cannot be protected without security. In a practical sense, this means at inception, the collection of personal data must be minimized such that only the information that is needed and that we have a legal basis for, should be collected and stored. In each stage, the data should be encrypted and accessible only on a need-to-know basis by authorized individuals who have been appropriately authenticated. At the end of the lifecycle, GDPR compliant approaches should be adopted so that if a DSAR request exercising the right to be forgotten or the right to erasure comes through, it can be fulfilled. In such a case, the flow of new content should be stopped, and existing personal data should be securely and permanently destroyed.

- Visibility and Transparency
    - Visibility and transparency are needed to demonstrate accountability with regulators and to establish trust with clients, customers as well as with Omnicom employees. This includes, but is not limited to:
        - making our privacy policy and associated privacy notifications available to the appropriate audiences.
        - requiring adequate privacy protections contractually when transferring personal data through a third party; and
        - ensuring compliance with regulations which includes active monitoring, privacy risk assessments, internal audits and confirming compliance with this policy.

- Respect for User Privacy:
    - At the core of privacy regulations is the notion that privacy is a fundamental right. This must be kept in mind during the planning and design phase. This means not only taking the least intrusive approach by processing only what is necessary and lawful, but consciously designing user-centric systems that make it easy for the user to manage his/her personal information. This includes but is not limited to:
        - Obtaining consent to collect and disclose personal data where appropriate;
        - Storing and maintaining personal data that is accurate and up to date;
        - Enabling users to challenge the accuracy and completeness of their data; and
        - Configuring privacy by default settings.

2.10 Privacy risk assessments

Data is the lifeblood of advertising and media marketing companies. To build marketing campaigns, service our clients and support our own employees, we must take measures to protect confidential, sensitive and personal data. Such measures include conducting risk assessments to better understand our level of compliance; this is needed in order to make informed decisions about managing or mitigating identified risks. Further, privacy risk assessments enable us to spot non-compliant processes and procedures so that we may address them and thereby avoid regulatory fines. Omnicom and its Agencies shall use the following privacy risk assessments when appropriate:

Data Protection Impact Assessments (DPIA)

A data protection impact assessment (DPIA) is an ongoing process that is designed to minimize the risks that are associated with processing personal data. DPIAs should be conducted if there is a possibility that the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. DPIAs are required only when the data that is collected is subject to GDPR (remember that noncompliance with GDPR can lead to substantial fines). If you are working on a processing activity in the UK or EU that involves personal data, please reach out to your DPO and/or DPL to find out if a DPIA is needed. A sample DPIA can be found here .

Privacy Impact Assessment (PIA)

Privacy impact assessments (PIAs) focus on how PII data (see section 1.3 for a definition), is collected, used, shared and maintained. Typically, a PIA is required at the start of a new project, new process or when a new service or product that requires the processing of personal information is launched. However, a PIA should also be applied when changes are made to the way we handle the processing of personal information for an existing project, product or service.

When possible, PIAs should be done in the planning stages and certainly prior to deployment. If you are working on a project or processing activity that involves personal information, please reach out to your local DPO and/or DPL to find out if a PIA is needed; do this as soon as possible to avoid potential rework or redesign.

Privacy risk assessment templates will be created by OMC's Global DPO(s) and/or Global DPL(s) and approved by Legal. However, the obligation to carry out these assessments ultimately rests with Agencies (and their DPOs/DPLs). Further, OMC's Internal Audit team will conduct its own assessments to gauge how well agencies or project teams are complying with the guidelines and principals that are laid out in this Policy.

2.11 Data Retention

Data privacy laws impose obligations on us in relation to how long we store personal data. Generally, we should only retain personal data so far as it is (a) required for an ongoing legitimate business purpose (including financial, tax and legal record keeping purposes) or (b) where a specified retention is required by clients pursuant to a contract, law, regulation or a court order.

To comply with this principle, we are implementing a Data Retention Policy and Schedule that will govern how long different categories of data should be retained within Omnicom and in what situations these periods might be extended. However, given the global nature of our business and the multitude of local laws that can govern the retention of certain records, this Retention Policy and Schedule can

only ever be a guide. If local laws in your jurisdiction require or prohibit retention of data for a period that differs from the retention schedule that is outlined in this policy, you should discuss it further with your DPO or DPL. It is not the intention of this policy to override local laws and regulations. Similarly, Agencies should follow the Data Retention Schedule, but it may be necessary to adapt based on local laws, practices and additional data types or use cases that may be relevant to your Agency.

Biometric authentication is permitted only when biometric data is processed and stored exclusively on the user's device in line with Omnicom's endpoint security controls

2.12 Complying with Lawful Requests for Information

Omnicom and its Agencies will comply with all court orders and enforceable subpoenas that request information, including PII data, on its network and systems. This is typically referred to as a "legal hold". During the course of legal action, Omnicom will protect the requested data from being deleted. You may not destroy evidence or circumvent measures taken to protect lawful requests for this information.

- You will be informed if data, including emails, needs to be preserved for legal investigations.
- You may be required to provide information on any legal or regulatory matter that you are involved in.
- You may be required to provide your work computer or mobile device (if used to access work related emails) in order to comply with legal investigations.

2.13 Training

Omnicom will provide privacy awareness training modules. The curriculum offered will be based on global regulations e.g., GDPR, Canada's PIPEDA, Brazil's LGPD, California's CCPA and HIPPA. The content will be short, concise and offered in multiple languages. When nominated, you must satisfactorily complete the training.

It is the responsibility of DPOs and/or DPLs to ensure that training is carried out. Further, DPOs and/or DPLs will follow up on the status of privacy awareness training. If you are an employee, your completion status will be provided to your manager. If you are a contractor, consultant or an employee of a vendor who has access to our data, your training completion status will be provided to your business sponsor. Please contact your DPO or DPL if you have any questions that are specific to privacy training.

PART 3 – Governance Information and Policy Management

3.1 Responsibility

The Omnicom Information Risk Management Committee ("IRMC") is responsible for the administration of this Policy. If you have any questions regarding this Policy or if you have questions about items not addressed in this Policy, please contact your DPO or DPL.

3.2 Review

The following procedures shall be applied to the documents that govern the OMC Privacy Program:

- This Policy shall be reviewed each year by DPOs and DPLs
    - Updated versions shall be reviewed by the stakeholders of the program before they can be published, with final approval being given as per the section "Changes to this Policy" below.
- Procedure documents shall be reviewed by DPOs and DPLs

3.3 Policy Distribution

This Policy will be made available to all employees periodically and provided to new joiners via the Privacy Channel IT Central (a privacy centric document repository).

3.4 Changes to this Policy

This Policy is a living document. As such, it will be occasionally reviewed and updated to maintain applicability and alignment with Omnicom's business practices as well as applicable laws and regulations.

Revisions of this Policy will be presented to the Information Risk Management Committee ("IRMC") for review and approval. Revisions of the document shall supersede all previous versions.

The signatures of at least two members of the IRMC are needed to authorize any material revision. Authorizations are set out at Part 4 below.

3.5 Exceptions to this Policy

Exceptions can only be made to this Policy with specific authorization approved by the IRMC.

Typically, exceptions to this Policy can only be made in very limited circumstances and will only be granted following a review by the IRMC.

Exception requests related to the inability to comply with this Policy must be made via the Omnicom's Risk Acceptance Request Form that can be found on the Paige Service Portal or by clicking here.

All requests for deviations from the policies and standards require a risk exception submission. All approved exceptions are documented and retained with acceptance rationale and the timeframe for which the exception shall apply. The exception request evaluation is based on the potential risk to the Agency and Omnicom. Exceptions shall be granted for no longer than one year at which time they must be resubmitted, if applicable.

3.6 Administration of this Policy

Omnicom expressly reserves the right to change, modify, or delete this Policy's provisions. The IRMC is responsible for the administration of this Policy. If you have any questions regarding this Policy or if you have questions about items not addressed in this Policy, please contact your DPO or DPL as previously noted in this document.

PART 4 - Authorizations

The Information Risk Management Committee of Omnicom has reviewed these policies and concur that they align with our fundamental business goals and professional ethics. In good faith and with all due authority, we, the undersigned, sign these policies into effect, the effective date being noted in the revision table. The Policy is authorized and enforced as part of our normal daily operations.

SCHEDULE 1 – UK/EU Data Subject Rights

Please note for the purpose of this Schedule “Omnicom” “we” or “our” or “us” means the relevant Omnicom or Agency entities within the scope of the Request and “you” means the person responsible for actioning the Request as per Part 2 above.

1. The Right of Access

Individuals have the right to have access to and a copy of all personal data that we hold and processes about them

Information may be required before responding to an access request
The scope of the searches
If it is not clear from the Request what personal data the requestor seeks to obtain, you will need to confirm the scope of the searches you will carry out for that individual's personal data. Omnicom or the relevant Agency will be expected to make extensive efforts to search for all information that the requestor wishes to obtain and cannot request that the requestor narrow the scope of the proposed searches. However, Omnicom or the relevant Agency are not required to do anything that would be unreasonable or disproportionate while taking into account the fact that the right of access to personal data is regarded as a fundamental right for individuals to have control over their personal data.

When sending the requestor confirmation of the Request, you should confirm the scope of the searches to be carried out that will give the requestor the opportunity to respond if they believe that alternative or additional searches would be appropriate.

You may wish to propose specific search terms to the requestor. Generally, these will be the name of the requestor, along with a reasonable date range. This will allow electronic documents to be searched quickly.

The following considerations may be relevant when determining the scope of the search:

- date ranges: if there is a particular matter that the requestor is interested in, a limited date range while that matter was active may be more appropriate. However, the requestor can insist on receiving personal data from any date range;

- local hard drives: in most cases it will be appropriate to ask individuals within the business who hold relevant information to conduct a search for that information within the search parameters, rather than conducting a remote IT search. This will help limit and focus the amount of data returned in the course of the search. In a small number of instances and where it is necessary to preserve the confidentiality of the requestor, you may decide it is not appropriate to inform any individuals whose documents will be searched. However, this will mean that searches can only be made of documents on shared network drives rather than local hard drives. In the event that the requestor makes a complaint to a data protection authority, you may be required by that authority to carry out searches of local hard drives, and the individuals whose hard drives are to be searched would then have to be informed that these will be searched;

- deleted and backed-up data: data protection authorities will not expect Omnicom to provide personal data that has been deleted. In respect to back-up data, if you are satisfied that the back-up replicates the data held in live systems, it is unlikely that a data protection authority would require specific searches of back-up data;

- archived data: archived data should be searched, as data protection authorities generally deem this to be data that the controller has decided it may wish to retrieve at a later date. The exception is where this archived data is difficult to retrieve and would therefore be very unlikely to be used to make decisions about an individual;
- hard copy documents: hard copy documents that are stored in such a way that information about individuals is readily accessible are within the scope of an Access Request. This could include an HR file about that individual, although it would not include notes made by individuals in a personal notebook, unless they were taken with the intention of turning them into an electronic record.

When is an Access Request valid?

Access Requests made by an individual for information that relates to that individual are always valid. However, controllers are not obliged to respond to repeated requests that are made at unreasonably frequent intervals. If Omnicom receives frequent or numerous requests from the same individual, you should take into account whether the personal data is particularly sensitive, whether the processing might affect the requestor's rights and whether the personal data is likely to have changed since the last request, before determining whether the interval between requests is unreasonable. In some cases, there may be scope for charging a fee to respond (i.e., where the request is “manifestly unfounded or excessive”), although this will not always be the case.

Further information relevant to carrying out an Access Request

As well as the documents held in hard copy or electronic form, the scope of the searches may refer to information held by third parties such as service providers. In this case, you should consider whether third parties may be holding information to which you would not have access. This might include information from service providers who have access to HR data that you do not have direct access to, for example.

After the searches are carried out, the documents returned should be reviewed as quickly as possible to ensure that time limits are adhered to. As part of this process, you should redact or withhold information that is exempt from disclosure. All queries regarding the review exercise should be referred to your DPO, DPL or legal support. The following considerations may be relevant to the review process:

- if the documents contain any personal data of individuals other than the requestor, this information should normally not be disclosed. This information should be redacted or withheld in order to provide only the personal data of the requestor. It should only be disclosed if the other individual has consented to its disclosure;
- if information is subject to privilege, for example, personal data is included in legal advice provided to Omnicom, or has been prepared by lawyers in reasonable anticipation of litigation, it should not be disclosed to the requestor;
- if personal data is included in information that relates to the prevention or detection of a crime, it should not be disclosed if doing so might prejudice the investigation into that crime;
- where personal data is included in management forecasting or planning, that personal data does not have to be provided if providing it would prejudice any of Omnicom's business activities. For example, if there is a list of names for proposed redundancies including the individual making the Request, this would be likely to prejudice our conduct, so would not need to be disclosed;
- records of Omnicom's intentions in relation to negotiations with the requestor do not have to be provided where release of that information would be likely to prejudice those negotiations.

There are also other exceptions relating to confidential references, corporate finance, publicly available information, armed forces, ministerial appointments, examination scripts and self-incrimination.

Note that the bullets above set out exemptions to the right of access that apply primarily in the UK under current data protection law. In other EU jurisdictions there may be alternative exemptions that apply, and certain exemptions listed above may not apply. The exemptions that are applied must be in line with local applicable law and you should discuss these with your DPO.

What must we provide in response to an Access Request?
You should provide an individual making an Access Request with:

- a copy of all the personal data that is disclosable (with any exempt or irrelevant information removed); and
- a copy of the privacy notice relevant to the requestor. If this is not available or it would be easier, the cover letter could be populated with the required information (specified in Article 15 of the General Data Protection Regulation).

2. The Right of Rectification

Individuals have the right to require Omnicom to rectify their personal data to the extent that it is inaccurate (a "Rectification Request"). For example, if an individual changes his or her name, we must update their records on receipt of a Rectification Request.

Individuals also have the right for any personal data that is incomplete to be updated (e.g., by supplementing with additional, accurate information), considering the purposes of the processing.

Information that may be required before responding to a Rectification Request
Upon receipt of a Rectification Request, you should verify that the personal data provided as a correction to existing personal data is actually correct.

If required, further information should be requested from the individual who made the Rectification Request, and they should be informed of what information would be required to verify the changes, and for Omnicom to comply with the Rectification Request.

When is a Rectification Request valid?
If the information that Omnicom has on file is incorrect, and the updated information provided by the requestor is correct as described above, a Rectification Request is valid.

Further information relevant to carrying out a Rectification Request
You should ensure that any entities processing the personal data subject to the Rectification Request are informed of the updated personal data. The operational steps for records to be updated to reflect changes under a Rectification request will depend on the nature of the specific request received. This might include circulating the updated details to relevant departments (e.g., IT and HR), inputting changes to employee databases, etc. Different procedures may be required for different categories of individual, e.g., employee personal data is likely to be updated in a different way from consumer or service provider personal data. This is not required if it would be impossible or take disproportionate effort.

What must we provide in response to a Rectification Request?
The confirmation that the relevant information has been corrected or updated should be communicated to the requestor so that the individual is aware that the changes have been made.

If requested, Omnicom must also provide a list of all the entities that have received the personal data and that have been contacted by us as described above.

3. The Right of Erasure

Individuals have the right to require Omnicom to delete their personal data in certain circumstances.

Information that may be required before responding to an erasure request
If it is not clear from the Erasure Request, you may need to verify precisely which personal data the requestor wishes to be erased, and it may also be helpful to understand why the requestor wishes to have that information erased.

When is an Erasure Request valid?
Omnicom must delete personal data on receipt of an Erasure Request where:

- the personal data is no longer necessary for the purpose for which it was collected. For example, if a contact of a business partner no longer works for that business partner, there would be no need to retain that information as the information was originally collected for processing in the context of that relationship;
- the personal data is processed only on the basis of the consent of the requestor, and the requestor withdraws that consent. In general, making an Erasure Request would be considered a withdrawal of consent;
- the requestor objects to processing (as described in section 6 below), and there are no overriding legitimate grounds for Omnicom to carry on the processing;
- the personal data is being processed unlawfully, for example if Omnicom was processing personal data on the basis that it was necessary for the performance of a contract with the requestor, but that contract has now been terminated and there is no other reason to keep the personal information; or
- the personal data must be erased to comply with a legal obligation to which Omnicom is subject.

Omnicom is **not** required to delete personal data that is subject to an Erasure Request where the processing of the personal data is necessary:

- for exercising the right of freedom of expression and information.
- for compliance with a legal obligation to which Omnicom is subject or for the performance of a task carried out in the public interest. For example, if Omnicom is required to maintain records relating to business partners for purposes of mandatory disclosures to tax authorities for a certain period, it would not be required to erase the personal data of those business partners within the required period;
- For reasons of public interest in the area of public health. This is unlikely to apply to Omnicom;
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, and only if erasing the personal data would be likely to render impossible or seriously impair the achievement of these objectives; or
- For the establishment, exercise or defense of legal claims. For example, Omnicom would not be required to delete personal data about a former employee with whom there is an existing employment dispute.

Further information relevant to carrying out an Erasure Request

Considering the costs of implementation, Omnicom should ensure that any entities processing the personal data subject to the Erasure Request are informed of the erasure. The operational steps for records to be updated to reflect changes under an Erasure Request will depend on the nature of the specific request received. This might include circulating the updated details to relevant departments (e.g., IT and HR), inputting changes to client databases, etc. Bear in mind that different procedures may be required for different categories of individual, e.g., employee personal data is likely to be updated in a different way from consumer or service provider personal data. This is not required if it would prove impossible or involve disproportionate effort.

What must we provide in response to an erasure request?

Once a request by an individual to delete their personal data has been implemented, you should contact the requestor to inform them that his or her personal data has been deleted.

If requested to do so by the requestor, we must also provide a list of all the entities that have received the personal data, and that have been contacted by us as detailed above.

4. The Right to Data Portability

Individuals have the right to request that personal data that they have provided to Omnicom is provided to them in a commonly-used digital format, and they have the right to request that this information be sent to another data controller in certain circumstances (as explained below) (a "**Portability Request**"). The impact of this right will likely be limited in the context of our operations (i.e., it will only be in limited circumstances, if any, where a Portability Request is valid).

Information that may be required before responding to a Portability Request

You may wish to contact the individual to confirm which organisation or organisations his or her personal data should be transmitted to, including the means by which this personal data should be transmitted.

When is a Portability Request valid?

Individuals have the right to receive their personal data in a commonly used digital format, and they have the right to request that this information be sent by Omnicom to another data controller where:

- the processing of that personal data is carried out on the basis of:
  - the consent of the individual; or
  - on the basis that it is required for the purposes of fulfilling a contract to which the individual is a party.

It is therefore important that you identify the lawful basis upon which Omnicom has collected or processed the personal data that the requestor has requested.

- the processing is carried out by automated means, for example, processing subscription payments made by consumers for a monthly OTT streaming service where credit card payments will be processed automatically each month; and
- where the information has been "provided to" Omnicom by the requestor. This includes:
  - personal data that has been actively and knowingly provided by the individual (e.g., by supplying his or her name, age, postal address, email address, payment information on a form); and
  - personal data that has been generated by the requestor using the controller's goods or services, or that the controller has observed about the requestor's use of goods or services (e.g., cookie data, viewing history, location data).

Further information relevant to carrying out a Portability Request

You should compile the personal data about the requestor that meets the requirements set out above. The operational steps required to extract data that is subject to the right to data portability might include running a script to extract particular categories of personal data from databases. You should also consider the format that the data should be extracted into. This should be an open format that retains as much metadata as is practicable, while also being sufficiently abstract from any proprietary data formats that might reveal information about the ways that Omnicom operates its systems, for example, XML, JSON or CSV. You should also ensure that the format is sufficiently abstract to not reveal any of Omnicom's intellectual property rights or trade secrets.

What must Omnicom provide in response to a Portability Request?

Omnicom must provide the requestor with a copy of all the information that is subject to the right to data portability in a commonly used digital format. The appropriate format in a particular circumstance will depend on the specific request that has been made, but the relevant format should be an open format that retains as much metadata as is practicable, while also being sufficiently abstract from any proprietary data formats that might reveal information about the ways that Omnicom operates its systems.

In responding to a Portability Request, you must ensure that such actions do not adversely affect the rights of others. You should not transmit personal data of other individuals.

5. The Right to Restriction of Processing

Individuals have the right to request that the processing activities that Omnicom carry out with respect to their personal data are restricted in certain circumstances described below (a "Restriction request").

Information that may be required before responding to a Restriction Request

If it is not clear from the Restriction Request, you should confirm which uses of personal data the requestor wishes to restrict.

When is a Restriction Request valid?

A Restriction Request will be valid where:

- the accuracy of the personal data is disputed by the individual making the Request;
- the processing is unlawful, but the individual does not wish to have the personal data erased, and wishes to restrict its use instead;
- Omnicom no longer requires the personal data for its own purposes, but the individual requires the personal data for the establishment, exercise, or defense of legal claims; or
- the individual has objected to the processing (see section 6 below), and you are in the process of verifying whether its legitimate interests override those of the individual.

If a Restriction Request is found to be valid, Omnicom will not be able to process the individual's personal data other than where the individual has consented to the processing, for the establishment, exercise or defense of a legal claim, to protect the rights of another person, or for reasons of important public interest to the EU or a Member-State.

Further Information relevant to carrying out a Restriction Request

Considering the costs of implementation, you should ensure that any entities that carry out processing activities that were subject to the Restriction Request are informed of the erasure. This is not required if it would prove impossible or involve disproportionate effort. The operational steps required for records to be updated to reflect the processing that can no longer take place after a Restriction Request will depend on the circumstances. As an example, this might include flagging certain data points relating to an individual to ensure they are not processed in a particular manner. Bear in mind that different procedures may be required for different categories of individual, e.g., employee personal data is likely to be updated in a different way from consumer or service provider personal data.

What must Omnicom provide in response to a restriction Request?

Omnicom must inform the requestor that the processing of his or her personal data has been restricted in line with his or her request and provide details of the processing activities that have ceased.

If requested by the requestor, you must also provide a list of all the entities that process the relevant personal data and that have been contacted as detailed above.

6. Right to Object to Processing

Additional information that may be required before responding to an Objection Request

If it is not clear from the Objection, you should clarify which uses of personal data the requestor is objecting to.

When is an Objection valid?

Upon receiving an Objection from an individual, Omnicom must cease carrying out the processing activities that relate to the individual's personal data and which the individual has Objected to when:

- the processing activity in question takes place on the legal basis of Omnicom's "legitimate interests" and there are no compelling legitimate grounds to override the interests of the requestor;
- the processing takes place for the purposes of carrying out direct marketing activities (such as sending marketing emails, letters, SMS messages or push notifications). In this case, Omnicom should immediately cease those direct marketing activities.

If, however, Omnicom is required to keep the personal data in order to make or defend legal claims (for example, if a former employee is making a claim), an Objection Request would not be valid.

Further information relevant to responding to an objection request

The operational steps required for records to be updated to reflect the processing that can no longer take place after a valid Objection Request will depend on the circumstances. This might include flagging certain data points relating to an individual to ensure they are not processed, for example. Bear in mind that different procedures may be required for different categories of individual, e.g., employee personal data is likely to be updated in a different way from consumer or service provider personal data.

What must Omnicom provide in response to an objection?

Omnicom must inform the requestor that the processing of his or her personal data has ceased in line with their Objection, and in particular provide details of which processing activities have ceased.