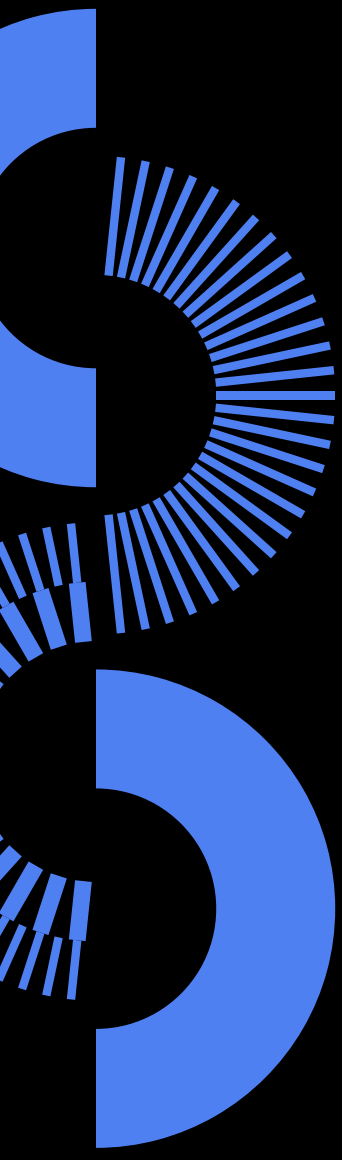
OMNICOM

DATA RETENTION AND RECORDS MANAGEMENT POLICY

UPDATED 2024

CONFIDENTIAL —
NOT FOR EXTERNAL
DISTRIBUTION



Contents

PART 1 – Introduction

1.1. Overview

This Data Retention and Records Management Policy (the "**Policy**") establishes the principles, procedures and best practices for determining how long Omnicom Group, its Networks, Agencies, Affiliates, Associations, and Subsidiaries ("Omnicom and Agencies") retain personal data and other business information ("**Records**"). It describes the role and responsibilities of Omnicom and Agency personnel and the processes that should be followed at the Omnicom and Agency level.

1.2. Audience and Scope

This Policy applies to anyone performing services for or on behalf of Omnicom and Agencies (a "Covered Person"). 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). 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 and it is possible that in some circumstances, local Data Privacy Laws, regulations, or government guidance may conflict with provisions of this Policy. In the event of such conflicts, the Data Privacy Laws should prevail over this Policy.

Practice Groups and Agencies should also put in place their own data retention policies as necessary to supplement the requirements of this Policy.

1.3. Related policies

This Policy must also be read and understood in conjunction with the following policies:

- Global Security Policy, Omnicom User Information Security Manual and any other policies relating to information security.
- Global Data Protection and Data Privacy Policy.
- Guidelines on how to classify documents and Data.
- Acceptable Use Policy.

These policies and procedures can be found on the intranet via the following link: https://oneomnicom.sharepoint.com/sites/OMC-ITCentral/SitePages/Policies.aspx

1.4. 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 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, in particular 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, and in some cases this may be narrower than the above. However, for the purposes of this Policy – and to ensure the best possible data governance standards – 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".

- **"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.

- **"Records"** includes information recorded in any medium, including, but not limited to, any hardcopy or electronic writing (including, without limitation, e-mail), fax, voice mail, instant message, drawing, graph, chart, photograph, audio or video recording, computer application or other data compilation that (i) is created, received or maintained by any Covered Person in that person's business capacity, (ii) relates to Omnicom or Agency or its business, and (iii) is in the possession, custody or control of the Omnicom or Agency or a Covered Person. Please note that Records that are located in your home or at any other offsite location are subject to this Policy and must be handled accordingly. **Some Records may include personal data (see above), however not all will - some will contain only business information.**

- **"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.

1.5. Wording Conventions

Throughout this Policy, 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.

1.6. Compliance/Enforcement

Breach or 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 is committed during or outside office hours and whether or not the breach takes place at your normal place of work. You will be required to co-operate with any investigation into a suspected breach, which may involve providing us with access to any relevant device and any relevant passwords and login details.

PART 2 – Record Management Policy

2.1. Objective

This Policy and the procedures included in this Policy are designed to ensure that:

- the Records (as defined below) of both Omnicom, Agencies and documents of external origin are created, managed, classified, and disposed of in accordance with applicable legal and regulatory record-keeping requirements our business needs; and
- Control and ensure you maintain the latest (either by date or version number), original up to date version of all relevant documents, including documents of external origin.
- Omnicom and Agencies satisfy their legal duty to retain and preserve materials that have been or might be requested in a pending or anticipated legal proceeding, audit or investigation.

Creating, managing, classifying, and disposing of Records in accordance with this Policy will make relevant information more readily accessible for legitimate business use, avoid the unnecessary retention of duplicate Records and reduce expenses by eliminating the storage of unnecessary and outdated Records.

The Policy along with the Retention Schedule does this by establishing rules and guidelines for organizing, retaining, and disposing of Records, including personal data. It sets out:

a) the principles by which we have determined how long Records should be retained for, and when they should be deleted;
b) the specific retention periods in place for different types of Records, across the different jurisdictions in which we operate; and
c) guidance on appropriate Record handling and disposal.

This Policy is intended to set out the main principles by which Omnicom and Agencies determine how long Records should be retained for and when they should be deleted. Guidance as to how this applies to different types of Records can be found in the Retention Schedule linked to at Annex 1. This sets out relevant retention periods for (a) different business functions and (b) different jurisdictions.

This Policy and Retention Schedule applies to all Omnicom and Agency entities in the following markets:

- US
- UK
- France
- Germany
- Netherlands
- Italy
- Spain

For other markets, the US periods in the Policy and Retention Schedule can be used to set a "baseline" for record retention. However, there will be instances where retention periods need to be varied to comply with local laws and regulations and so local advice may be needed before implementation.

This Policy only applies to personal data where Omnicom or Agencies are the data controller. Where Omnicom or Agencies process personal data on behalf of clients, they are obligated to retain the personal data as instructed by that client or as required by applicable law.

2.2. Policy implementation

Omnicom or Agency Data Protection Officers ("DPOs") are responsible for the implementation of this Policy within the Agencies or Business Units or Practice Areas for which they are responsible. DPOs may delegate responsibility for implementation to Agency Data Privacy Leads ("DPLs") if necessary.

The Retention Schedule will be reviewed annually and revised in accordance with changes in legal requirements or business needs. If you become aware of a conflict between a retention period provided

in the Retention Schedule and the law, please resolve it by adhering to the law and notify your DPO so that a correction in the Retention Schedule can be made promptly.

2.3. Our general approach to Record Retention

The governing principle of the Policy is this: we should only retain records as far as they are:

(a) required for a legitimate business purpose (including financial, tax and legal record keeping purposes); or

(b) where a specified period of retention is required by law, regulation, or court order.

Subject to the exceptions in 2.4 - if a Record is not needed for these purposes, it should be disposed of in accordance with Part 3 of this Policy.

As noted above Data Privacy Laws (including the GDPR/UK GDPR) provide that personal data must not be kept for longer than necessary (under the Storage Limitation Principle). At the same time, retaining Records (many of which contain personal data) is necessary to run our business, for regulatory compliance, for accounting, tax and legal purposes, and in order to protect our legitimate interests.

To balance these competing concerns, we have put in place a Retention Schedule to govern how long Records are kept for. Because there are potentially tens of thousands of individual Records, we have made a choice to apply retention periods to Record categories or types (although the Retention Schedule will give an idea of the specific Records that fall within each category). A retention period is then applied to each Record category. The specific retention period will vary according to the nature of that Record category.

Retention periods will be dependent on:

- the type of Records and the original purpose;
- whether we would expect to use the Records for a different purpose in the future (for example, where the Records may be necessary to defend against possible legal claims, they will be retained for the duration of relevant legal limitation periods or, where they are relevant for accounting or tax purposes, they will be kept for an appropriate period given that need); and
- whether Omnicom or Agencies are *required* to keep the Record under relevant local laws or regulations (which can often be the case for some financial, health and safety and employment Records).

2.4. Using our Retention Schedule – further detail and exceptions

The Retention Schedule sets out the retention periods we apply to different categories of Record. These may vary across various locations.

Generally, Records should not be retained for longer than the retention period set out in the Retention Schedule. Upon expiry, the Records should be deleted (following the guidance in the section "Review and Deletion of Records" below).

In particular cases, we may have to retain Records for longer than the period set out in the Retention Schedule. Reasons for retaining Records for longer than the period set out in the Retention Schedule can include:

a) where a client contract or statement of work requires retention for a certain period (e.g., to satisfy client MSA audit requirements).

b) where there is a threat of litigation in relation to a specific matter or where the Records contain information relevant to a legal action which has already started or is in contemplation, in which case a legal hold may be put on the Record and must be complied with. See "Legal Hold Policy and Procedures" below; or

c) where statutory exemptions apply or where applicable laws, regulations, government agencies, certification bodies or self-regulatory organizations require further retention.

As above, whilst Omnicom has made every effort to capture such requirements in the Retention Schedules, it acknowledges that the periods set out cannot cover all local variations and it is not intended that the retention periods override applicable local law. In particular, if the Retention Schedules contradict local law or regulation, or government or regulatory guidance, the latter shall prevail.

Longer retention on the above grounds should be approved by the relevant Omnicom or Agency DPO.

Please note that certain temporary items need not be retained in accordance with the Retention Schedule. These temporary items are described below in the Section entitled "**Review and Deletion of Records.**"

2.5. Legal Hold Policy and Procedures

When the Office of the General Counsel, or (as relevant) the appropriate legal counsel for your Agency or Practice Group, (hereafter and collectively just called "Legal") becomes aware that a legal proceeding, audit or investigation is pending or anticipated, it will promptly notify the appropriate persons and direct that any Records pertaining to that proceeding, audit or investigation be labelled for retention until further notice (a "legal hold"). The legal hold could take the form of an e-mail, a hard copy memo or a combination of these methods.

If you receive a legal hold or otherwise become aware that Omnicom or the Agency is the subject of any pending or anticipated legal proceeding, audit or investigation with respect to which you have pertinent Records, you ***must preserve those Records by immediately ceasing any alteration, deletion or destruction of such Records – even if under the current Retention Schedule, or otherwise under this Policy, you would be authorized to do so.*** This obligation is not limited to financial documents and associated Records, but includes many other types of Records, including those that you may have in your files (both hard copy and e-mail and other electronic files). In addition to the Records that you normally retain, you should also retain anything that might be relevant, such as copies, personal or convenience notes, etc. If you are in doubt about whether you have Records that pertain to a given matter, please ask the relevant Legal contact.

If you learn that a legal proceeding, audit or investigation is anticipated or has been commenced that has not been brought to your attention, please notify Legal immediately. ***DO NOT RESUME NORMAL DESTRUCTION PRACTICES ON ANY PERTINENT RECORDS UNTIL YOU HAVE RECEIVED FORMAL WRITTEN NOTIFICATION FROM LEGAL. In some cases, local laws may criminalize the destruction or alteration of Records with the intent to obstruct a proceeding. The penalties for this may include fines and imprisonment.*** In addition, Covered Persons who fail to preserve a Record subject to a legal hold notice may be subject to a disciplinary action, up to and including termination of employment or services.

In practice, users subject to a legal hold will have email deletion suspended for the duration of the notice.

2.6. Review and Deletion of Records – further guidance

The Retention Schedule sets out our standard retention periods for different types of Record. Unless an exception applies, Records should be kept for no longer than the retention period set out in the Schedule unless there is an appropriate reason for doing so. Records that have passed the period set out in the Retention Schedule should be deleted.

DPOs are responsible for implementing a process for regularly reviewing Records and identifying those that have passed their retention period. This process may entail delegating responsibility to DPLs but also to Covered Persons, whilst providing support/oversight as needed.

When reviewing records for deletion, please bear in mind the following:

- As the retention periods are often based around the relevant limitation periods for legal action it is generally permissible to leave a 6 month period after expiry of the relevant retention period before deletion occurs, to cover the possibility of late service of claims. However, this does not apply to "short retention" items (such as applicant data).

- Particular care should be taken when considering deletion of Records that are relevant to a client contract, or where retention may be required by law. **Final signed agreements and original Records should be retained (either electronically or in hard copy) in the central files of your department in accordance with the Retention Schedule**.
- When deletion is required, the relevant Records (in all forms, including electronic versions and hard copies) should be promptly disposed of by means appropriate to their nature or level of confidentiality, such as by purging, degaussing[1], shredding, or otherwise destroying the Records so they are unreadable or undecipherable and cannot be reconstructed. Particular care should be taken in relation to Records that are classed as Confidential or Restricted under our Data Classification Policy. ***Please note that when destroying hard copy personnel records, or other documents containing personal data you must ensure they are disposed of via an approved supplier, such as Iron Mountain (or if there is no approved supplier ensure they are otherwise securely shredded).***

- If you have any questions about whether to retain an item, do not retain it in your files indefinitely. The key to a successful Records Management Policy is its consistent application. Ask the relevant

[1] the process of decreasing or eliminating a remnant magnetic field so that data stored on magnetic media such as hard drives cannot be recovered.

DPO or DPL whether it is appropriate to retain the item and, if not, promptly dispose of it. If you accidentally dispose of an item that should have been retained, immediately contact your DPO or DPL / IT support to determine how to proceed.

- If you have received a legal hold notice from Legal, as described below in this Policy in the section entitled "**Legal Hold Policy and Procedures**", do not destroy any Records or temporary documents pertaining to that notice.

Temporary items/ non-records

Please note that certain temporary items are disposable as soon as they are no longer of use to you (unless a legal hold has been issued). These include:

- Emails that do not constitute a Record under the Retention Schedule. This would include emails that are only required temporarily - such as informal arrangement for an internal catch up, or emails relating to personal matters.
- Copies of Records that you are certain have been retained in their original form;
- Drafts of Records that are now complete.
- Printouts taken for ease of reference and note taking.
- Records that are widely available to the public; and
- Notes taken for personal use or convenience.

2.7. Records Integrity

Records frequently go through many changes before reaching their final form – and sometimes even after that. Drafts are prepared, updates are made and corrections are often required. Compromising the integrity of a Record, however, such as fraudulently "backdating" a document, is a very serious offense. Falsifying information in a Record is a violation of this Policy and the Omnicom Code of Business Conduct. In addition, tampering with a Record to impair its availability for use in an official proceeding may violate local law and may be punishable by fines or imprisonment.

If you discover that a Record in final form is incorrect, please correct it in a manner that makes clear why the change was made and the reason for that change. Please check with the relevant DPO / DPL for the approved procedure. Never "backdate" or otherwise enter incorrect dates on any Record with the intention of misrepresenting the actual date of creation or execution. If you have questions regarding the correct date to use for a Record, please check with the relevant DPO / DPL or Legal.

2.8. Applying retention periods to Email and Electronic Records

Within Omnicom Inc, e-mails are automatically deleted from the Inbox, Drafts, and Sent Items folders in the Company's e-mail system 90 days after they are received or sent, and from the Deleted Items folder 7 days after they are placed there (although this may vary at a regional or Agency level).

This means that to affect the retention periods in the Retention Schedule, positive action is required by each user to file the email in an appropriate location. A similar process may need to be followed when saving documents into our systems – i.e. you may need to ensure that the document is saved into an appropriate location that supports retention for the applicable period. This process may differ at the Agency level – please speak to your DPO/ DPL or IT support.

The creator of an e-mail is responsible for retaining that e-mail. However, if an e-mail was created by a non-Covered Person and it is a Record that needs to be retained, each Covered Person who receives the e-mail must retain it (unless otherwise directed by Legal).

When applying the above, please note that the vast majority of e-mails do not qualify as Records; and emails that are not Records should be promptly deleted. On the other hand, failure to retain e-mails that are Records can have serious consequences and result in the imposition of substantial penalties. If you are not sure what to do with a specific e-mail or other electronic Record, check with the relevant DPO / DPL before you click delete or elect to save it indefinitely.

2.9. Paper Records

Many paper Records will need to be archived before their retention period expires. DPOs are responsible for ensuring that there are adequate arrangements in place for this at an Agency level. When it is appropriate to move Records to off-site storage for archiving, the Records should be stored in such a way that it is clear what the Records are, the year they were created, the date their retention period expires, and the Covered Person or department responsible for the Records.

Archived Records are still subject to the retention periods set out in the Retention Schedule - archiving is not the same thing as deletion! As such, DPOs must ensure that periodic reviews take place in respect of archived Records, and where retention periods have expired they are deleted (where appropriate) in accordance with this Policy.

2.10. Termination of Employment/Discontinuance of Services

A Covered Person whose employment is terminated for any reason, or who has ceased to provide services to Omnicom or Agency shall turn over properly retained Records to his or her supervisor prior to departure, unless otherwise instructed. In addition, the IT department must be notified at least one week prior to departure, if possible, in order to ensure that the submission of such person's electronic devices and any electronic files which must be retained separately proceeds smoothly.

If a Covered Person is terminated without notice and the procedure above cannot be followed, such person's supervisor shall be responsible for ensuring that all Records are handled according to this Policy.

Please contact your Human Resources department for additional information regarding the procedures that should be followed in the event of a termination of employment or services.

2.11. Training

All Covered Persons are required to undergo training in the implementation of this Policy.

2.12. Interpretation and Assistance

The relevant Omnicom or Agency DPO is responsible for interpreting the provisions of this Policy and the Retention Schedule. Questions regarding this Policy should ordinarily be addressed to the DPO (or, if applicable, the DPL).

PART 3 – Governance Information and Policy Management

Created	[] November 2021
Last Reviewed	October 2024
Version	1.1.
Scope	See Part 1 above.
Location(s)	Applicable worldwide
Review By	Omnicom Information Risk Management Committee

3.1. Responsibility

The Omnicom Information Risk Management Committee is responsible for the administration of this Policy.

3.2. Policy Distribution

This Policy will be provided to new joiners, either by their local HR or IT Support. The Policy can always be found on the intranet.

3.3. Changes to this Policy

The Policy is a living document. As such, it will be periodically reviewed and updated to maintain applicability and alignment with Omnicom business practices and applicable laws, regulations, and guidance.

Revisions of the document 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 Information Risk Management Committee are needed to authorize any material revision. Authorizations are set out at Part 4 below.

Revision History

Version	Date Signed	Date Issued	Description
1.0	2021-11		
1.0	2022-08	2022-08	Policy Review
1.1	2023-06	2023-06	Updated section 2.1 regarding management of documents of External Origin
1.1	2024-10	2024-10	Annul review- No changes made

3.4. 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 inability to comply with this policy must be made via the Omnicom Risk Exception Request process workflow within the Paige Service Portal

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.

3.5. Administration of this Policy

Omnicom expressly reserves the right to change, modify, or delete this Policy's provisions. The Omnicom Information Risk Management Committee is responsible for the administration of this Policy.

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.

Paul Scott
Global Chief Information Security Officer

Craig Cuyar (Oct 4, 2024 10:32 EDT)

Craig Cuyar

Global Chief Information Officer & Senior Vice President

Annex 1 – Record Retention Schedule

The Omnicom Record Retention Schedule can be found on IT Central in the Security Policies folder located here: Security Policies (sharepoint.com)