

Policy & Schedule	Data Retention
Scope	<i>This policy <u>applies</u> to team members and volunteers</i>

1. Purpose

The data we hold at Canteen is vital for our business operations and the management of our team members and volunteers. We are legally required to keep some of this data for a certain period. We also keep data to support our business activities and to ensure information is readily available when needed. However, not all data is kept indefinitely. Particularly, data that includes personal information has extra legal responsibilities. Under the Australian Privacy Principles (**APP 11**), part of the *Privacy Act 1988*, we must take reasonable steps to destroy or de-identify personal information that is no longer needed for any purposes allowed under these principles. This is unless the law, a court order, or if the information is part of a Commonwealth record, requires us to keep it.

Keeping data can pose risks and costs to our organisation. This Data Retention Policy (**Policy**) outlines our approach to keeping and disposing of data. It should be read along with the *Data Retention Schedule* in Schedule 1. Not adhering to this policy could lead to fines, negative publicity, challenges in providing necessary evidence, and hinder our business operations.

This policy is not a part of any employment contract and can be changed at any time.

2. Principles

Principle	Definition
Privacy and confidentiality	Personal and sensitive information will be collected and stored in accordance with privacy legislation and regulation.
Legal requirements and standards	Adhering to laws and regulations established by the government and other regulatory bodies to ensure safety, well-being, and ethical standards are maintained
Leadership and Commitment	Canteen management will demonstrate active leadership and commitment to compliance, setting the tone for the entire organisation

3. Policy

3.1 Retention Periods

Data is required to be retained in accordance with the following requirements:

3.1.1 Formal or Official Records

Any Data that is part of any categories listed in the *Data Retention Schedule* contained in Schedule 1 to this Policy, must be retained for at least the amount of time indicated in the *Data Retention Schedule*. If a record contains Personal Information it must not be retained beyond the period indicated in the *Data Retention Schedule*, unless a valid legal or business reason (including a notice to preserve documents for contemplated litigation or other special situation) calls for

continued retention. If you are unsure whether to retain a certain record, contact the Data and Business Systems team in the Operations Department.

3.1.2 Disposable Information

The *Data Retention Schedule* will not set out retention periods for Disposable Information. This type of Data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of in accordance with Paragraph 5.

If Data is not listed in the *Data Retention Schedule*, it is likely that it should be classed as Disposable Information. However, if you consider that there is an omission in the *Data Retention Schedule*, or if you are unsure, please contact the Data and Business Systems team.

3.1.3 Personal Information

The *Privacy Act* requires us to take reasonable steps to protect Personal Information (including Sensitive Information) and to destroy or de-identify Personal Information once it is no longer needed for any purpose for which it may be used or disclosed under the APPs (subject to legal requirements for retention of the Data, other laws and where personal information is contained in a Commonwealth record). More information on how we use personal information can be found in our *Privacy Policy*.

3.2 Storage, back up and disposal of data

3.2.1 Storage

Our Data must be stored in a safe, secure, and accessible manner. Any document and financial files that are essential to our business operations must be duplicated or backed up at least once per week and maintained off-site, or both.

3.2.2 Destruction

Our Data and Business Systems team is responsible for the continuing process of identifying the Data that has met its required retention period and supervising its destruction or de-identification. The destruction of confidential, financial, and team member or volunteer related hard copy Data must be conducted by secure shredding. Non-confidential Data may be destroyed by recycling. The destruction of electronic Data must be coordinated with Data and Technology.

3.2.3 De-identification

The Data and Business Systems team may determine that Personal Information should be de-identified as opposed to destroyed as outlined in paragraph 5.2. In such circumstances the Data and Business Systems team will oversee the de-identification of Personal information in accordance with the Office of the Australian Information Commissioner's best practice guidance.

3.3 Preservation of documents for contemplation litigation and other special circumstances

The destruction of Data must stop immediately upon notification from the Operations division that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation. Destruction may begin again once the relevant Executive Team member lifts the requirement for preservation.

We require all team members and volunteers to comply fully with our *Data Retention Schedule* and procedures as provided in this Policy. All team members and volunteers should note the following general exception to any stated requirements of a destruction schedule: if you believe, or the Operations department informs you that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit or other event, you must preserve and not delete, dispose, destroy or change those records, including emails and other electronic documents, until the Operations division determines those records are no longer needed. Preserving documents includes suspending any requirements in the *Data Retention Schedule* and preserving the integrity of the electronic files or other format in which the records are kept.

If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the Operations team.

In addition, you may be asked to suspend any routine Data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

3.4 Where to go for advice and questions

Any questions about this Policy should be referred to the Risk and Compliance Lead who is in charge of administering, enforcing and updating this Policy.

3.5 Breach reporting and audit

3.5.1 Reporting Policy breaches

We are committed to enforcing this Policy as it applies to all forms of Data. The effectiveness of our efforts, however, depends largely on team members and volunteers. If you feel that you or someone else may have breached this Policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor dealt with the matter properly, you should raise the matter with the relevant Executive of the area involved. If team members and volunteers do not report inappropriate conduct, we may not become aware of a possible breach of this Policy and may not be able to take appropriate corrective action.

3.5.2 Reprisals

No one will be subject to and we do not allow, any form of discipline, reprisal, intimidation or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or cooperating in related investigations.

3.5.3 Audits

The Risk and Compliance Lead in conjunction with the Executive will review this Policy every three years and its procedures (including where appropriate by taking outside legal or auditor advice to ensure that we are in compliance with relevant new or amended laws, regulations or guidance). Additionally, we will regularly monitor compliance with this Policy.

3.6 Regulatory breach notification requirements

Certain actual or potential breaches of this Policy will require us to make formal notifications to government regulators in Australia. If you become aware of or suspect such a breach has occurred or are unsure if a breach has occurred, you should inform your supervisor immediately or raise the matter with the relevant Executive of the area involved to ensure that we adequately fulfil our compliance obligations in accordance with our *Data Breach Response Guideline*.

4. Responsibilities

4.1 All Canteen team members

All Canteen team members are responsible for complying with:

- this Policy and the *Data Retention Schedule*
- any communications suspending Data disposal, including the destruction or de-identification of Personal Information
- any specific instructions from the Data and Business Systems Team and the Operations department.

Failure to do so may subject us, our team members, and contractors to serious civil or criminal liability, or both. A team member's failure to comply with this Policy may result in disciplinary sanctions, including suspension or termination. It is, therefore, the responsibility of everyone to understand and comply with this Policy.

4.2 Risk and Compliance Lead

In addition to Section 4.1, the Risk and Compliance Lead are responsible for advising on and monitoring:

- compliance with this policy
- data protection and data retention laws which regulate Data, including personal information.

5. Definitions

- **Confidential information belonging to others:** any confidential information that a team member or volunteer might have obtained from a source outside of Canteen, such as from a previous employer or organisation, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted or destroyed.
- **Data:** all data that we hold or have control over (including, for example data held by our hosting and service providers in cloud or offsite records storage) and therefore to which this Policy applies. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both Personal Information and Non-personal Information. In this Policy we refer to this information and these records collectively as Data.
- **Data Retention Schedule:** Schedule 1 attached to this Policy which sets out retention periods for our Formal or Official Records.

- **Disposable Information:** consists of Data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose or Data that may be safely destroyed in accordance with Paragraph 5.2 because it is not a Formal or Official Record as defined by this Policy and the Data Retention Schedule.
- **Formal or Official Record:** certain Data is more important to us and is therefore listed in the Data Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. We refer to this as Formal or Official Records or Data.
- **Health Records:** health information collected in connection with the provision of a health service.
- **Personal Information:** any information or an opinion about an identified individual or an individual who can be reasonably identified from the information or opinion. Information or an opinion may be Personal Information regardless of whether it is true (section 6, Privacy Act). It includes special categories of Personal Information such as health information (see Sensitive Information).
- **Sensitive Information:** a sub-set of Personal Information defined under the Privacy Act which includes health information. Sensitive Information is subject to a higher level of privacy protection under the Privacy Act and additional obligations are imposed on organisations under the APPs with regard to the collection and handling of Sensitive Information.

6. Appendices

6.1 Schedule 1 – Canteen Data Retention Schedule


7. Related documents

Legislation	<ul style="list-style-type: none"> • <i>Privacy Act 1988</i> • <i>Australian Privacy Principles</i> • <i>Corporations Act 2001</i>
National Safety and Quality Digital Mental Health Standards	<ul style="list-style-type: none"> • <i>1.31 Transparency</i>
National Principles for Child Safe Organisations	1: Child safety and wellbeing is embedded in organisational leadership, governance and culture
Internal policies, procedures and supporting documents	<ul style="list-style-type: none"> • <i>Privacy Policy</i> • <i>Personal Information Consent Form</i> • <i>Whistleblower Policy</i> • <i>Charter of Service User Rights</i> • <i>Service User Records Policy & Procedure</i> • <i>Information and Data Security Policy</i> • <i>Databreach Guideline</i> • <i>Digital Disaster Recovery Procedure</i> • <i>Internet and Business Communication Tools Policy</i>

8. Governance

Canteen Policy: OD016- POL Data Retention Policy and Schedule 1112023

Location: Policy Library > Operations > Data & Technology

Effective date	30/11/2023	Review date	30/11/2026
Policy owner: Executive Director, Operations		Endorsement Level: Executive	
Endorsement Signature		Printed Name	

Schedule 1 – Canteen Data Retention Schedule

Canteen establishes retention or destruction schedules or procedures for specific categories of data. This is done to ensure legal compliance (for example, with our data protection obligations) and to accomplish other objectives, such as protecting intellectual property and controlling costs.

Team members and volunteers should comply with the retention periods listed in this schedule, in accordance with the [Canteen Data Retention Policy](#).

If you hold data not listed in this schedule, please refer to the [Canteen Data Retention Policy](#). If you still consider your data should be listed, if you become aware of any changes that may affect the periods listed below or if you have any other questions about this Data Retention Schedule, please contact the Risk and Compliance Lead.

*A reference to a **limitation period** in the tables below refers to the limitation periods contained in the relevant state and territory limitations acts (for example in NSW the *Limitation Act 1969* (NSW)). This legislation sets out the deadline for filing a claim in certain matters (e.g. breach of contract or personal injury), it is important for Canteen to retain this information for the length of the relevant limitation period in the event a legal claim is brought.

1. Company and corporate records

TYPE OF DATA	RETENTION PERIOD	COMMENTS
Accounting records.	Seven years after the transactions covered by the records are completed.	<ul style="list-style-type: none"> Sections 286, 287, 288, 289 and 1306, <i>Corporations Act 2001</i> (Cth) (CA 2001). Best practice. <p>Tax requirements or other legislation may require longer. Note also that if records are kept in electronic form, they must be convertible into hard copy and available within a reasonable time.</p>
Register of members, debenture holders or option holders.	Indefinitely. Entries for former members can be removed seven years after the date they ceased to be members.	<ul style="list-style-type: none"> Sections 173(1) and 169(7), CA 2001. Best practice. <p>A company is required to allow any person, whether a member or non-member to inspect its registers.</p>
Minutes of meetings of directors or	Indefinitely.	<ul style="list-style-type: none"> Section 198F, CA 2001. Best practice. <p>The CA 2001 does not specify the</p>

TYPE OF DATA	RETENTION PERIOD	COMMENTS
members.		<p>period for which minutes of meetings must be kept. However, as meetings are the official written record of the business transacted at a meeting, minutes should be retained permanently.</p> <p>Note also that current and former directors have a statutory right to inspect the books of the company (including the company's minute books) for the purposes of legal proceedings. These rights continue for seven years after the person ceases to be a director of the company.</p>
Historical records and archives about the company, for example, former directors, chairpersons and officers of the company.	Indefinitely.	<ul style="list-style-type: none"> • Usual practice. • No set period in law. <p>It may be advisable to retain this information for historical purposes in the legitimate interests of the organisation.</p>
<p>Australian Charities and Not-for-profits Commission (ACNC) reporting information including:</p> <ul style="list-style-type: none"> • Financial records; and • Operational Records (e.g. evidence of ACNC and tax compliance and evidence of entitlement to be registered as a charity). 	Seven years after the transactions, operations or acts covered by the records are complete	<ul style="list-style-type: none"> • Section 55-5, Australian Charities and Not-for profits Commissions Act 2012 (Cth). <p>Several states no longer require separate reporting for fundraising activities where Canteen is registered with and reporting to the ACNC. To the extent that a state or territory's record keeping requirements are not covered in Section 3 (Fundraising Records) this retention period should apply to fundraising information.</p>

2. Fundraising Records

TYPE OF DATA	RETENTION PERIOD	COMMENT
<p>NSW fundraising information including:</p> <ul style="list-style-type: none"> Record of participants; Cash books; Register of assets; Register of receipts; Record of minutes. 	<ul style="list-style-type: none"> Accounting records Other records: Three years 	<ul style="list-style-type: none"> <i>Charitable Fundraising Act 1991</i> (NSW) NSW Charitable Fundraising Guidelines
<p>ACT fundraising information including:</p> <ul style="list-style-type: none"> record a true and fair view of income and expenditure; and keep records in a way that allows them to be conveniently and properly audited. 	Seven years	<ul style="list-style-type: none"> <i>Charitable Collections Act 2003</i> (ACT) <p>If the collection is part of a collection that is carried out both inside and outside of the ACT, it's not necessary for the records to identify the amount obtained within the ACT. The whole collection amount can be identified.</p>
<p>VIC fundraising information including:</p> <ul style="list-style-type: none"> financial records; Primary financial accounts; and Summary financial accounts. 	Three years	<ul style="list-style-type: none"> <i>Fundraising Act 1998</i> (Vic) <p>If the fundraising was part of a national fundraising activity, Canteen does not have to prepare summary accounts specific to Victoria.</p>
<p>Records of communications with State and Territory fundraising regulators, including notices of fundraising activities.</p>	Seven years	<ul style="list-style-type: none"> Limitation period* <p>Several States still require Canteen to meet certain obligations when fundraising, such as providing notice of the fundraising activities. Records should be kept of these notices or any requests from regulators.</p>

3. Team member and Volunteer Records

TYPE OF DATA	RETENTION PERIOD	COMMENT
Records of team members as prescribed by regulation,	At least seven years after termination of	<ul style="list-style-type: none"> Section 535, <i>Fair Work Act 2009</i> (Cth) (FW Act).

TYPE OF DATA	RETENTION PERIOD	COMMENT
such as date of commencement, employment contract, pay, leave particulars and termination date.	employment.	<ul style="list-style-type: none"> Regulations 3.31 to 3.40, <i>Fair Work Regulations 2009</i> (Cth) (FW Regulations).
Record of any superannuation contributions on behalf of a team member.	At least seven years after termination of employment.	<ul style="list-style-type: none"> Section 535, FW Act Regulation 3.37, FW Regulations <p>Records of contributions made to certain defined benefit funds will have different requirements as are regulated by other legislation such as the <i>Superannuation Industry (Supervision) Act 1994</i> (Cth).</p>
Tax file numbers of team members.	Must take reasonable steps to securely destroy or permanently de-identify individual's tax file number information that is no longer required by law to be retained or is no longer necessary for a purpose under taxation law, personal assistance law or superannuation law.	<ul style="list-style-type: none"> Section 11(2), Privacy (Tax File Number) Rule 2015 (Cth)
Volunteer information including: <ul style="list-style-type: none"> volunteer name and contact information; records of any certifications, clearances or registrations necessary for their involvement (e.g. working with children checks); volunteer training information; and number of volunteers. 	Seven years from the end of the volunteer period	<ul style="list-style-type: none"> Limitation period*

4. Canteen service user information

TYPE OF DATA	RETENTION PERIOD	COMMENT
<p>Personal Information of Canteen service users including:</p> <ul style="list-style-type: none"> • name, contact details, date of birth and gender; • emergency contact details; • information provided via forms or survey responses that does not constitute sensitive information; • photographs; • enquiry/complaint details; • information about interactions with Canteen, including records of any telephone, email or online interactions. 	<p>Duration of the individual's involvement with Canteen plus seven years.</p>	<ul style="list-style-type: none"> • Limitation Period* • Privacy Act, APP 11
<p>Sensitive information of Canteen service users including:</p> <ul style="list-style-type: none"> • health information such as current and past medical history and assessments (excluding health information collected as part of a health service); • cultural background; • details of relationships; and • personal circumstances and other information that service users choose to provide. 	<p>Duration of the individual's involvement with Canteen plus seven years.</p>	<ul style="list-style-type: none"> • Limitation period* • Privacy Act, APP 11 <p>Sensitive information should only be retained as long as reasonably necessary for Canteen's purposes in accordance with APP 11.</p> <p>In the absence of any legal obligation to retain this data the Data and Business Systems Team in consultation with the relevant Executive should consider if an earlier destruction date should be applied noting the sensitive nature of the information and the potential harm caused if the information was involved in a data breach.</p>
<p>Health information collected in connection with the provision of a health service.</p>	<ul style="list-style-type: none"> • For Adults: seven years from the last occasion on which a health service was 	<ul style="list-style-type: none"> • <i>NSW Health Records Act 2002 (NSW), s 25(1).</i> <p>When health information is destroyed a record must be kept of the name of the</p>

TYPE OF DATA	RETENTION PERIOD	COMMENT
	<p>provided to the individual by the health service provider.</p> <ul style="list-style-type: none"> For Minors (under 18 years): until the individual has attained the age of 25 years. Record of destroyed health information – indefinitely. 	<p>individual to whom the health information related, the period covered by it and the date on which it was deleted or disposed of.</p> <p>Canteen may also have contractual obligations to retain health information for longer periods.</p>
<p>Records relating to Indigenous individuals, families or communities or to any children, Indigenous or otherwise, removed from their families for any reason.</p>	<p>Indefinitely with informed consent</p>	<p>Recommendation from the <i>Bringing Them Home report of the National Inquiry into the Separation of Aboriginal and Torres Strait Islander Children from their Families</i>, April 1997</p>
<p>Information relating to child sexual abuse or alleged abuse, including;</p> <ul style="list-style-type: none"> records containing information about the whereabouts of workers; records documenting actions taken to address allegations and cases of sexual abuse of children and related matters; and records documenting support to and remedial action for individuals who have alleged child sexual abuse. 	<p>45 years.</p>	<p>This period is recommended in recommendation 8.1 of the Final Report Recommendations: <i>Royal Commission into Institutional Responses to Child Sexual Abuse</i>, December 2017</p>

5. Facilities and information technology records

TYPES OF DATA	RETENTION PERIOD	COMMENTS
<p>Closed-circuit television (CCTV) recordings.</p>	<p>30 days for routine recordings.</p> <p>As long as necessary for any investigations or claims that arise.</p>	<ul style="list-style-type: none"> Business need Privacy Act, APP 11 Limitation Period* Australian Standard 4806-2006: Closed Circuit Television (CCTV) – Management and

TYPES OF DATA	RETENTION PERIOD	COMMENTS
		<p>Operation</p> <p>Recordings should only be retained as long as reasonably necessary for Canteen's purposes in accordance with APP 11.</p> <p>Note also New South Wales and Australian Capital Territory have an additional requirement to inform team members before recordings take place.</p> <p>Additionally, more complex requirements exist for recordings that include sound.</p>
Visitor logs.	Seven years.	<ul style="list-style-type: none"> • Limitation Period* • Privacy Act, APP 11
General information about internally developed information technology (IT) infrastructure, software and systems for internal use.	Five years from decommissioning of system.	<ul style="list-style-type: none"> • Business need <p>No statutory period</p>
General information about externally developed IT infrastructure, software and systems for internal or external use.	Seven years from decommissioning of system.	<ul style="list-style-type: none"> • Contractual obligation • Limitation period* <p>Information relating to externally produced IT systems should be retained for 7 years to protect against any contractual disputes.</p>
Systems monitoring (for example, to detect and prevent failures, vulnerabilities and external threats).	Seven years.	<p>There is no statutory requirement to retain this information however the Australian Government Signals Directory recommends that event logs be retained for 7 years.</p> <p>It is advisable for organisations to keep monitoring logs malware or malicious code may go undetected in a system for a long period of time.</p> <p>Where IT infrastructure,</p>

TYPES OF DATA	RETENTION PERIOD	COMMENTS
		software or systems are used externally (for example, by customers), monitoring logs might also be relevant to claims and disputes.
Business continuity and information security plans.	Seven years from when the plan is superseded.	<ul style="list-style-type: none"> • Business need. • Legal or contractual obligation. • Limitation period. No statutory period. Consider whether the organisation is subject to any legal or contractual obligations in respect of business continuity which might necessitate a longer retention period, for example when contracting with Government bodies it is not uncommon to see requirements for the creation and retention of such plans. Business continuity plans might also be relevant to claims and disputes.
System backups.	Six months by default unless an exception is included in the relevant policy or process	<ul style="list-style-type: none"> • Business need. • May be different depending on the system.

6. Sales, marketing and customer records

TYPE OF DATA	RETENTION PERIOD	COMMENTS
Bought in mailing lists and associated contracts.	One year for mailing lists. For associated contracts; seven years from expiry or termination (12 years for contracts executed as a deed).	<ul style="list-style-type: none"> • Best practice for mailing lists. • Limitation period for contracts. No statutory period. However, personal information should only be retained as long as reasonably necessary for Canteen's purposes in accordance with APP 11.
Customer and donor relations database	Seven years from last contact.	<ul style="list-style-type: none"> • Business need • limitation period

TYPE OF DATA	RETENTION PERIOD	COMMENTS
records (for example, call centre records, queries, meeting feedback and account history).		
Marketing opt-out or suppression lists	Indefinite.	<ul style="list-style-type: none"> • Business need • Spam Act 2003 (Cth) • Do Not Call Register Act 2006 (Cth) • Privacy Act APP 7 Only sufficient information to enable the opt-out should be retained.
Evidence of consent to marketing (including electronic marketing).	While consent valid. Seven years from date consent was withdrawn or ceases to be valid.	<ul style="list-style-type: none"> • Business need • Limitation Period* • Spam Act 2003 (Cth) • Do Not Call Register Act 2006 (Cth) • Privacy Act APP 7 Consent can be withdrawn at any time and may not necessarily remain valid indefinitely, although how long it remains valid will depend on the context.
Press releases.	Five years from publication.	<ul style="list-style-type: none"> • Business need
Customer complaints handling.	Seven years from settlement or closure.	<ul style="list-style-type: none"> • Business need • Limitation period*
Website analytics reports from cookies and other similar technology.	Two years.	<ul style="list-style-type: none"> • Business need. Cookies themselves may be set for different periods depending on the function of the cookie.

7. Legal records

TYPE OF DATA	RETENTION PERIOD	COMMENT
Contractual documents.	Contract period plus six years (12 years for contracts executed as a deed).	<ul style="list-style-type: none"> • Limitation period*
Previous versions of policies, including IT policy, privacy policy and retention policy.	Six years from being superseded.	<ul style="list-style-type: none"> • Limitation period* • Business need

TYPE OF DATA	RETENTION PERIOD	COMMENT
Insurance claims.	Six years after settlement of claim.	<ul style="list-style-type: none"> • Limitation period*
Records of each notifiable incident under work health and safety laws.	Five years from the day the notice of the incident is given to the regulator.	<ul style="list-style-type: none"> • Section 38(7), Work Health and Safety Act 2011 (Cth) • The relevant work health and safety legislation for the State or territory, for example Section 38(7), Work Health and Safety Act 2011 (NSW) <p>Australian businesses are required to notify the work health and safety regulator immediately becoming aware of any death, serious injury or dangerous incident arising out of the conduct of their business occurs.</p>
Intellectual Property Records including: <ul style="list-style-type: none"> • trademark applications; • patent records; and • moral rights waivers. 	Six years from expiry of the relevant right.	<ul style="list-style-type: none"> • Limitation period*