

RETENTION MEETS DATA PRIVACY

Balancing privacy considerations with legislative retention requirements and legitimate business needs

THINGS TO CONSIDER

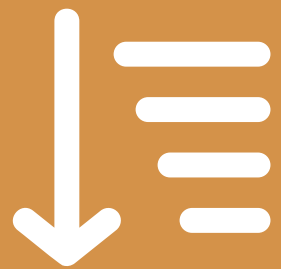
DEVELOPING RETENTION SCHEDULES

- Identify record/data categories containing personal information
- Consider where new types of records/data containing personal information fit into your retention schedule, or whether they require a new category
- Determine appropriate retention periods related to legal requirements, business needs, litigation risks and other key factors



DATA MINIMIZATION

- Retaining large quantities of data increases potential risk in the event of a breach and increases storage costs
- Only collect and retain personal information you require for a legitimate purpose
- Create a data inventory to better understand what personal information you have, where it resides and how it is classified
- Ensure personal information that is no longer needed is securely disposed of, redacted, segregated, or appropriately anonymized and/or de-identified



DATA TRANSFERS & STORAGE LOCATIONS

- Organizations remain accountable for personal information regardless of storage location
- Use data mapping to understand how personal information flows through your organization, where it is collected and potential points of transfer
- Consider where personal information is stored to understand which laws may apply
- Consider where 3rd Party Service Providers are headquartered in addition to where they store data



DEFENSIBLE DISPOSITION

- Proper disposition of records and personal information reduces the risk of legal liability and the potential for harm in the event of a breach
- Always conduct due diligence in determining appropriate retention periods and document your rationale
- It is not enough to have retention policies in place – you must practice active disposition of records and data
- Regulators want to see that you have considered the relevant factors, made a reasonable determination and have implemented it

