

DMA advice:
Data retention
2017



Contents

Introduction	2
Keeping data	3
Ranking your data	4
Engagement cycles	5
Creating a schedule	6
Putting it into practice	8
Deleting data	9
Conclusion	10

Introduction

Tackling the GDPR can be a little overwhelming. But with a little guidance and a closer look at exactly what it is your business holds, managing your personal data can be a perfectly manageable process.

Under the GDPR, businesses should not hold data for longer than is necessary, and they must have a legal ground in order to process any personal data for.

Organisations will have to decide on a series of policies for how long to hold customer personal data for, which will be dependent on the context.

The first step? A company must assess what personal data it already holds by carrying out a comprehensive data audit.

Not sure where to start? Check out our data audit infographic below.





Keeping data

The overarching principle of the GDPR is that a company must have 'Privacy by Design' at the core of its ways of working, policies and practices.

Put simply, an organisation must reassure its customers that it is working as hard as it can to protect their personal data. And rightly so.

A key principle of the new legislation is how businesses should not be keeping data for 'longer than necessary'. But what does this actually mean in practice?

A perfectly acceptable question with a perfectly acceptable answer.

First up, a business should be looking at what kinds of data they hold. From there, it is a case of asking how long you should be keeping this data for.

As your company probably holds several kinds of data e.g. employee, customer, supplier – the approach should be to set up different retention periods for each of these.

For example:

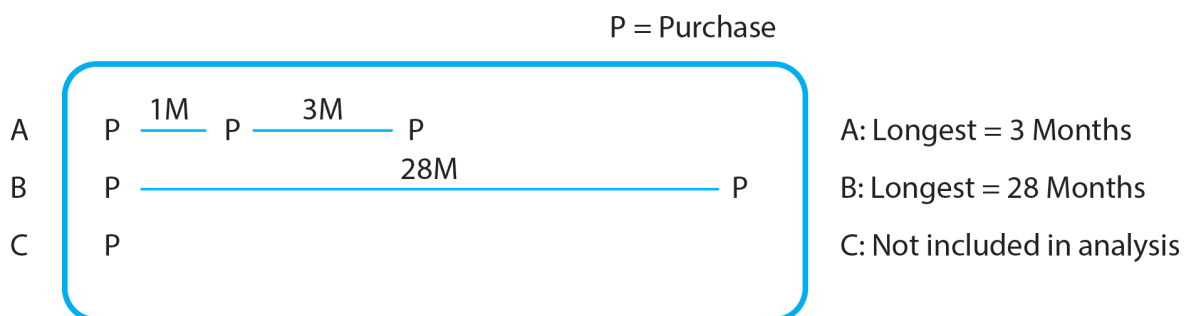
- You may need to retain some data sets for a specific period to comply with financial or other regulations.
- You may need to retain some indefinitely to support the services you offer e.g. unsubscribing from marketing communications or opting out of certain types of processing.
- You may need to keep some for as long as someone is actively engaged with your business e.g. users of an active subscription, contacts for an active contract, active subscribers to a service such as newsletters or jobseekers services.

Ranking your data

For many, the most difficult question to answer is 'how long after interacting with your business, can an individual be regarded as a customer?'

One way to answer this question is to look at the transaction history of current customers to measure their purchasing lifecycle.

Here is one method to help guide you: measure the 'interval' or 'gaps' between purchases and identify the longest inactivity period for each customer, as illustrated below for individuals A, B and C.



From here, you can then rank all of your customers based on the longest 'gap' in ascending order.

Then, simply count up the individuals from the top until you reach 90% of the population e.g. if you have 100 customers overall, this be the 90th in the ranking.

Look at the length of the 'gap' for this customer: that is the point in time when the probability of re-engaging 'falls below 10%'.

In the table below you can see measurements for the overall home shopping market, based on research performed by Epsilon Abacus:

% of Total Customers	Longest Interval to Next Purchase (in months)
10%	1
25%	4
50%	12
75%	27
90%	50

The research shows that after 50 months, 10% of customers still re-purchase.

This means that this retailer could argue that they have a legitimate reason to retain customer data for up to 50 months, as there is still a significant chance of the customer re-engaging with the brand.



Engagement cycles

Obviously, lifecycles vary by product category, so you should run an analysis using your own data before deciding how long to keep your customer data.

If you prefer a less mathematical solution, you can use your business knowledge.

For instance, some services may only have one-off or short engagement cycles e.g. single purchases, attendances at a one-off event, so a shorter retention period in these cases is probably appropriate.

For renewable products and services, it's sensible to set a retention period with the likelihood of renewals happening.

For datasets of prospective customers, the retention period is different.

It will change if they become active customers, but then, the typical sales cycle length is a good indicator of how long data should be kept.

An example of this would be if sales are normally closed within a three month window, keeping unclosed sales (open opportunities) for longer than six to twelve months is probably too long.

However, if the sales cycle can be anything up to one or two years, retaining this data for three years is too long.

Creating a schedule

A schedule is always a good idea, and is definitely best practice when approaching data of this scale.

Creating a data retention schedule means you can document your thought processes, in case you are audited by the ICO.

Below is a high level example of a retention schedule:

Sensitivity Level	Retention Period	Type of Record
Secret	Three years from end of fiscal year	Pay & tax: HMRC correspondence, PAYE records, maternity and paternity pay records
	10 years from end of fiscal year	Tax returns
	Five years from birth of child	Parental leave records
	Six years after last action	Employment records: redundancy, equal opps; health & welfare records; pay & tax: pay deductions, tax forms, payroll, loans
	30 years after employment ceases	Medical & health records
	life of company	Powers of attorney
Confidential	Three months from end of campaign	Call sheets, draw data
	One year after last action	Mailing lists, mailing proofs, interview records, unsuccessful job applications
	Two years from end of campaign	Fundraising agreements, call centre details, google analytics data
	Three years from last action	Fundraising stories, image consent forms, parental consent, consent forms, release forms, subject access requests, notifiable disease, insurance claims
	Six years from end of fiscal year	Accounting & financial management information, personal data (including coa), complaints, employment records, legacies, intellectual property, pay & tax, pension information, risk & insurance
	10 years from last action	Litigation dossiers, agreements/ contracts, declarations of interest, superannuation registers
	12 years after benefit ceases or adoption	Pensioner records, investment policies, statements of investments principles and policies
	15 years from last action	Building & maintenance contracts, licenses, leases
	50 years from expiry	Copyright material, patent applications

Internal Only	Two years from last action	Correspondence to unsuccessful grant applications, proposals and assessment forms. also all constitutional documents
	Three years after last action	Lotteries returns, time sheets, accident report forms
	Six years after last action	Asset registers, receipts, purchase orders, invoices - revenue, petty cash, creditor's & debtor's records; benefits in kind; draw results; standard T&Cs, itts, software licenses, management accounts, successful grant applications and correspondence, trade marks
	10 years after last action	Invoices - capital; supplier's details; insurance schedules
	12 years after last action	Signed contracts; guarantees & indemnities, riddor notifications; property dossiers
	20 years from purchase	Stock transfer forms and share certificates
	25 years	Property plans and surveys
	Unrestricted	Three months from end of campaign
One year after last action		Handbooks and guides to media relations, job advertisements
Two years from last action		Website FAQs, logo requests
Three years from last action		Annual return, job descriptions, raffle tickets
Six years from last action		Remittance advices, stock records, credit and delivery notes, pat tests, fire hazard tests
15 years from last action		Engineers reports, maintenance schedules
25 years		Conservation and architect's reports, maps
Life of company		Annual reports & accounts, press releases and cuttings, register of members, memorandum of association, register of directors and secretaries, employer's liability insurance certificates



Putting it into practice

So now you have a schedule, it's important that you:

- Collect date stamps that accurately indicate when the data was collected, when transactions occurred, when contracts began and are due to end, and when the data subject last engaged with you and you with them
- Make sure that systems and data owners know about your retention policy and what they need to do to comply with it e.g. encourage them to work out how they are going to delete or anonymise datasets at the end of retention periods. Could this process be automated or will it be manual? Whose responsibility is it? (Then make sure they actually do it).
- Make sure that your customers know how long you are going to keep their data. You can do this by either mentioning it in your privacy policy or using 'just in time' notices when you collect data online.

Remember, there isn't a right answer for how long you should keep your data.

You just need to be able to prove that you've written everything down, made a plan, and that you're sticking to it.



Deleting data

Concerns around complying with GDPR are leading some organisations to thinking they have delete all datasets at the end of retention periods.

If this were to happen, UK PLC would lose a huge amount of actionable data that could allow business to flourish in the future.

Instead of deleting data, it is worth considering anonymising or pseudonymising it.

Data protection law does not apply to 'data rendered anonymous in such a way that the data subject is no longer identifiable'.

In fact, fewer legal restrictions apply to anonymised data in general, so the anonymisation of personal data can help service business information needs in a privacy-friendly way.

But - and there is a but - using anonymised data isn't a free lunch.

You need to:

- Use your retention schedule to document which datasets are suitable for anonymisation and which should be deleted – you will need to justify your decision
- Keep assessing which datasets are suitable for anonymisation and monitor any new ones
- Train staff properly in anonymisation techniques

A good source of further reading is The University of Manchester's The Anonymisation Decision-Making Framework by Mark Elliot, Elaine Mackey, Kieron O'Hara and Caroline Tudor.



Conclusion

This guidance has been created to help organisations decide how they want to tackle data retention.

Ultimately, the final decision rests with the organisation.

Careful consideration to individual circumstances and context needs to be addressed from the get-go.

The key takeaways:

- Carry out an extensive data audit and then break it down into manageable chunks
- Make sure your business is accountable for their actions - document everything as you go along, a schedule is a good way of doing this
- Be transparent as possible with your customer, reassure them their data is safe with you – building trust is key to business success from May 2018 and beyond

If you have any questions regarding this piece of guidance, and you are a DMA member, then please get in touch with the [DMA's legal help desk](#).



Contributors

This DMA advice piece is produced by the GDPR hub of the [DMA's Data Council](#).

Liz Curry, business process manager, **Comic Relief**

Robbie Burgess, global data privacy programme lead, **RELX Group**

Michele Masnaghetti, head of analytics, **Epsilon Abacus UK**

With insight from DMA external affairs manager Zach Thornton and layout and design from the DMA's brand and content team.

About the DMA

A DMA membership will grow your business. Our network of more than 1,000 UK companies is privy to research, free legal advice, political lobbying and industry guidance. Our members connect at regular events that inspire creativity, innovation, responsible marketing and more. Most of them are free.

A DMA membership is a badge of accreditation. We give the industry best-practice guidelines, legal updates and a code that puts the customer at the heart. We represent a data-driven industry that's leading the business sector in creativity and innovation.

One-to-one-to-millions marketing attracts the brightest minds; individuals that will shape the future. By sharing our knowledge, together, we'll make it vibrant.

Published by The Direct Marketing Association (UK) Ltd Copyright © Direct Marketing Association. All rights reserved.

www.dma.org.uk





Copyright and disclaimer

DMA advice: Data retention 2017 is published by The Direct Marketing Association (UK) Ltd Copyright © Direct Marketing Association. All rights reserved. No part of this publication may be reproduced, copied or transmitted in any form or by any means, or stored in a retrieval system of any nature, without the prior permission of the DMA (UK) Ltd except as permitted by the provisions of the Copyright, Designs and Patents Act 1988 and related legislation. Application for permission to reproduce all or part of the Copyright material shall be made to the DMA (UK) Ltd, DMA House, 70 Margaret Street, London, W1W 8SS.

Although the greatest care has been taken in the preparation and compilation of *DMA advice: Data retention 2017*, no liability or responsibility of any kind (to extent permitted by law), including responsibility for negligence is accepted by the DMA, its servants or agents. All information gathered is believed correct at October 2017. All corrections should be sent to the DMA for future editions.