dataIQ™
Research report

GDPR suppression

dataIQ™ Whitepaper

Why data suppression is **key to compliance** with the General Data Protection Regulation

In association with

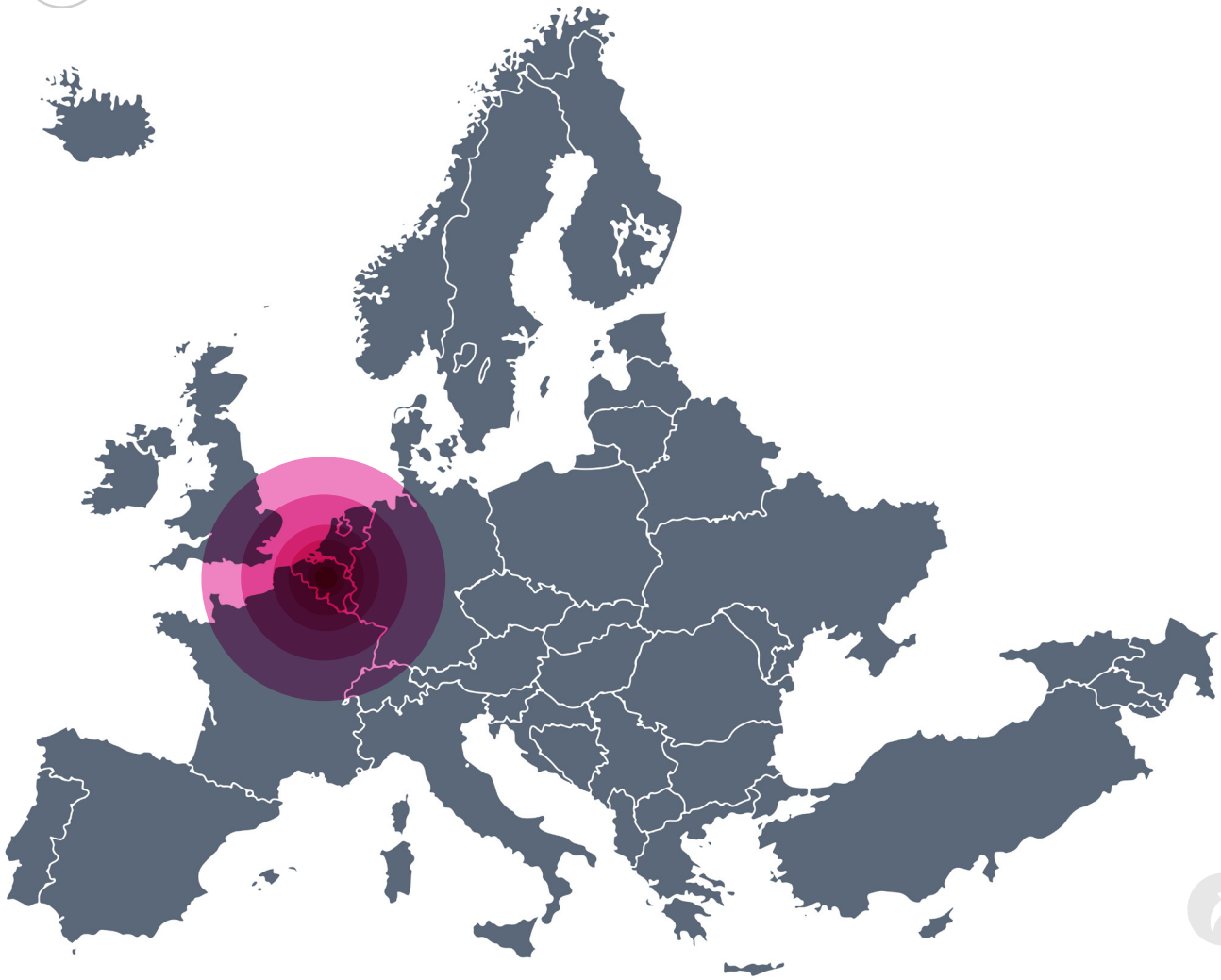
theark
DATA QUALITY SPECIALISTS

In association with theark DATA QUALITY SPECIALISTS

dataIQ™ Whitepaper

Why data suppression is key to compliance with the General Data Protection Regulation

Contents



1 GDPR - a warning from Brussels

Personal information is a regulated asset. That means any company which possesses it must comply with a set of rules about its capture, permissioning, management, transfer and deletion.

Those rules changed on 24th May 2016 when the UK adopted the General Data Protection Regulation (GDPR) which replaced the 18 year-old Data Protection Act. Organisations holding personal information have until 24th May 2018 to meet the requirements of the Regulation - after that date, the Information Commissioner's Office will start to enforce GDPR. That means potential fines of 2 per cent of global group turnover or €10 million for technical breaches of the Regulation and 4 per cent of global group turnover or €20 million for serious breaches. Every organisation which holds personal information is subject to GDPR - public sector, private sector, not-for-profit - and it expands the definition of personal information to new categories (such as location data and device ID) which means digital marketers need to pay attention. There is also no distinction made between data on individuals in a private or professional capacity, which means business-to-business marketers have to comply.

Two questions get asked by marketers when confronted with this risk. The first is whether UK organisations need to comply with GDPR given our impending exit from the European Union. This is easily answered - GDPR is already on the statute books, it just has not been enforced yet. When Brexit happens, all such European laws will be translated into UK law. Only

at some point in the future will the Government review which of these laws it might want to repeal. In order to trade with the EU after Brexit - including transferring personal information on European citizens - the UK will need to show it has laws in place which offer a similar level of data protection. Which means GDPR in all but name.

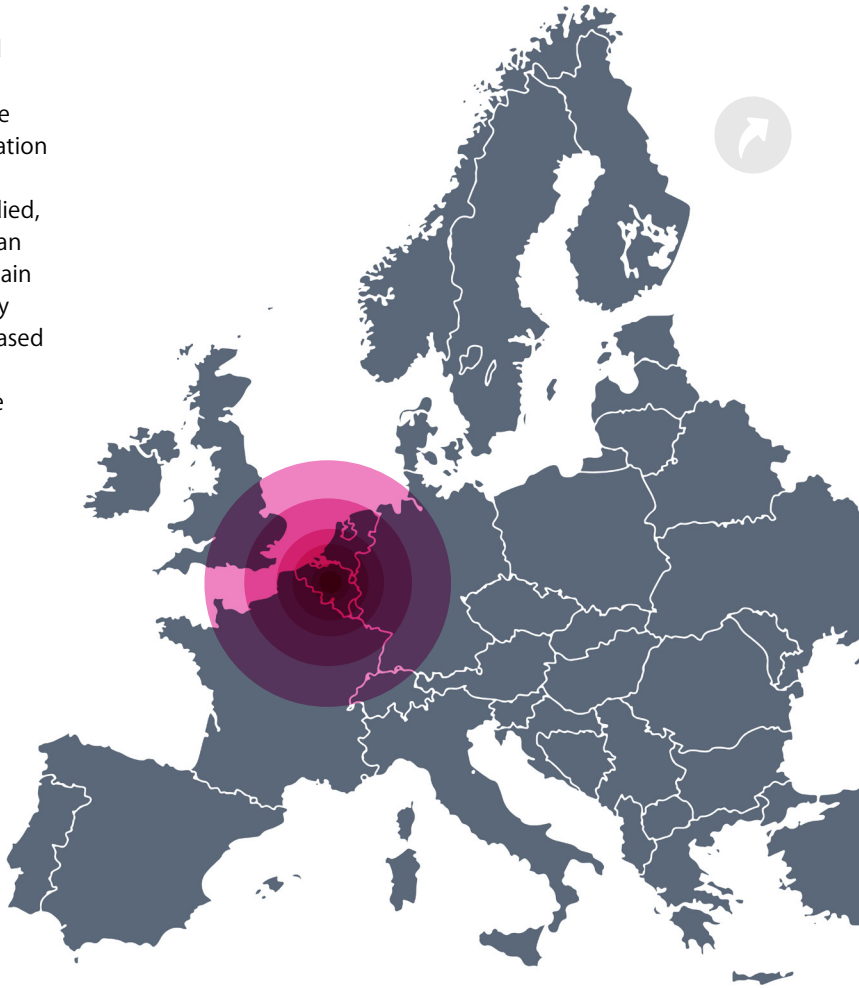
The second question may seem harder to answer - why should marketers worry about suppressing details of the deceased from their databases at all? After all, GDPR itself points out that: "This Regulation does not apply to the personal data of deceased persons." Superficially, this might seem to remove any obligation to run suppression files against customer databases and remove or flag those individuals who are known to have died.

But this assumption is not only false, it creates a very clear risk of a 2 per cent fine for a technical breach. This arises out of three main areas:

Accuracy - at the heart of GDPR is a requirement to ensure personal information is kept up-to-date and accurate and that any inaccuracies are corrected or erased as quickly as possible. The same article in the Regulation also makes it clear that personal information should not be kept for longer than the purpose for which it was originally acquired. If a customer has died, their data no longer serves any purpose (unless it can be shown that there is an ongoing obligation to retain their record) and should be suppressed. Equally, any customer database which contains records of deceased individuals can not be claimed to be accurate and up-to-date (if there is no purpose for keeping those deceaseds on file). That represents a clear technical breach of the Regulation which the ICO is likely to frown upon.

Demonstrating compliance - being able to show to the regulator that best efforts have been made to meet the demands of GDPR is not only best practice, it also reduces risk. One way organisations will need to do this is by documenting the type of data they store and what processes they use to maintain it. If suppression is not part of that maintenance, it will raise a doubt about how well data on the living is being processed and protected.

Breach notification - a new requirement of GDPR is to notify individuals in the event that data has been lost or stolen. This is meant to happen without undue delay and only those living persons at risk should be identified. If an organisation has not suppressed or flagged the deceased in its customer database, it will clearly not be able to meet this requirement. Suppressing in the wake of a data breach is the wrong time to take action.



2 Suppression, compliance and the business opportunity

Any investment into data management should be capable of demonstrating a positive benefit which not only offsets the cost, but also delivers an uplift against a specific measurement. Suppression is often viewed solely as a line of cost within marketing budgets. This is to alter the perspective against which its impact should be measured. If the full picture is viewed of where data is used - and therefore where data errors and poor quality databases will have an impact - then it becomes clear that suppression makes a positive contribution to the organisation and its marketing, just as much as targeting, segmentation and audience selection.

Campaign performance uplift - the outcome of any marketing campaign (digital or physical) is assessed against the total level of input activity. Suppose you are planning a direct mail campaign to a file of 1 million consumers and your target is a response rate of 1 per cent. If that file was representative of the UK population, is not more than 12 months old and had not been screened for deceaseds, then around 0.8 per cent of those records could be for people who are not living. That means starting with 800 records that can not deliver any response. While small in relative terms, that number multiplies according to how old the target file is, the age group being targeted (and its risk profile). As a result, the potential response rate is reduced right from the start. Removing those deceaseds and replacing them with living prospects resets the campaign metrics from a more positive base.

More accurate models - all types of marketing use models for decision making, from likelihood that an anonymous site visitor belongs to a particular demographic group through to propensity to respond and forecasts of customer lifetime value. Decisions on whether to invest in an activity need to identify the break-even point. If the customer base being modelled has not been screened for deceaseds, there will be an assumption about the potential gross volume which sets that break-even point in the wrong place - usually below that which is realistically achievable since the available base is actually smaller than assumed. Suppression will ensure the data entering models is up-to-date, leading to more accurate models and fewer decisions to pursue unprofitable actions.

Risk mitigation - GDPR has a very clear path towards compliance for any organisation holding personal information. It states: "In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default." By using suppression on a regular basis, data protection gets designed-in since it ensures living persons in the database are clearly identifiable and their rights can be supported. There is also a commercial benefit from maintaining data and regularly screening for deceaseds. Fraud can be reduced by having a clear indicator that a customer is no longer alive, thereby creating a barrier to criminal activities such as account takeovers or identity theft.

Customer engagement and reputation management - consumers judge every organisation against the best-in-class, regardless of industry sector. Those not able to achieve and maintain best in class standards will eventually lose market share. Leaders in data management are already establishing online control centres that allow customers to update and correct their personal information. The next step in that process is to have a clear protocol for handling deceased notifications. Even where customers are less likely to inform an organisation directly that a relative has died, fair processing notices should explain that suppression is used which will identify deceased individuals within a clear timeframe. That will reassure living relatives that the brand understands the distress which is caused by marketing to the deceased. Unless you want your brand to appear in the headlines for its insensitivity, suppression should become best practice as part of reputation management.

3 Reviewing your suppression strategy

A major impact of GDPR is to remove responsibility for the compliant handling of personal information from the domain of any one function. If, as a marketer, you have been used to setting your own strategy for whether to screen out deceased records (or not), the Regulation switches that decision up to enterprise level. Even the smallest of companies will have to address compliance, for example, because they hold employee records which are regulated. Large enterprises will make GDPR compliance part of their risk strategies.

That means a GDPR compliance project will start to look at any areas of the organisation's use of personal information and consider if there is exposure to a potential breach of the Regulation. Digital marketers who have chosen not to suppress email lists will need to explain to their board why they have taken that risk, for example. Individuals will no longer have the authority to place an entire organisation in non-compliance as a result of a refusal to screen databases.

Where a suppression strategy already exists, it will need to be reviewed to ensure it continues to be fit-for-purpose. That includes auditing all personal information stores and classifying the sensitivity of the data they contain. If this does not produce a legitimate business interest for retaining deceased customers' data, which would justify not applying suppression, then a programme for cleaning data - and keeping it clean - will need to be established. The frequency of cleansing and tolerance of matching will need to form part of this programme.

Where no strategy has been established - or an existing one has not been revisited for more than a year - an additional step is necessary. This should see providers of suppression files reviewed for their depth, quality, cost and capabilities in order to find the most appropriate partner. As is outlined in the next section, the answer to which provider to work with may not be the most obvious one.

Suppression strategy review - 22 point checklist

Data audit	• Location of records • Type of data • Sensitivity of data • Recency of data • Nature of permission gained • Date of permission gained • Date of last data cleanse
Data strategy review	• Purpose for which data is collected • Extent of purpose and legitimate interest • Duration of purpose • Retention/deletion lifecycle • Basis on which deceased data could be retained • Extent of exposed deceased data
Suppression provider review	• Market overview • Partner evaluation • Partner test • Partner selection
Suppression programme	• First pass suppression • Frequency rules • Matching rules • Evaluation of suppression • Metrics for uplift and impact from cleansed data

4 Suppression provider review: Why bigger is not always better

Suppression files have changed since they were first launched in the late 1980s. That is, some suppression file providers have changed the way they build their databases. This has resulted in a variety of file sizes being offered from the three leading providers, ranging from 5.4 million records up to 9.6 million. In a world where bigger is typically considered better, should total file size be the key consideration when reviewing providers?

So how does this difference in file sizes come about when the number of deaths occurring each year is an absolute? The answer lies in the steps which different vendors take to validate each record and therefore how they have chosen to build their file. Some files also contain very much older data. For example, some include records dating back to the mid 1980s, creating very large files as a result.

"In a world where bigger is typically considered better, should total file size be the key consideration when reviewing providers?"

Three types of data source are relied upon to build deceased files:

Probate data - any individual who dies leaving an estate with a value above £5,000 or who has made a will gets recorded via the probate system. This legal process is highly reliable, but also potentially slow - it can take up to nine months for a record to appear via this source.

Volunteered data - relatives of the deceased can notify a death to data owners via a number of routes, such as by completing a form provided to them by funeral directors. As this is entirely voluntary, it does not necessarily provide 100 per cent coverage and is also prone to human error and even misuse (such as registering as deceased to stop "junk mail", rather than registering with the marketing industry's preference services).

Derived data - certain actions and transactions will indicate that an individual has died, such as claiming on a life insurance or funeral policy. By comparing multiple data sources of this type, a high degree of confidence can be created in the validity of a deceased record. The more sources used to verify a record, especially from regulated sources (eg, FCA approved organisations), the more confidence can be gained.

When reviewing suppression file providers, especially for deceased records, it is important to look closely at how they have built their database, including:

- **Sources used**
- **Validation of records**
- **Confidence level**
- **Coverage**

Data evaluation - the golden key to your suppression strategy

If you are undertaking a review of your suppression provider, one critical component will make a huge difference - data evaluation. To be sure that a source file will deliver the performance you require, you need to run a test match against the target customer database (or a representative sample extracted from it).

Evidence gained from this type of test match will ensure that the final choice of suppression source is fact-based. It will also prove which file or combination of files will deliver the most effective and cost-efficient solution to your suppression requirements.

Data evaluation also helps you to avoid some of the common misconceptions about suppression. A few of these are:

- all suppression files are the same;
- you only need one suppression file;
- the bigger the file, the better it will perform.

If your organisation is choosing its provider based on one or more of these ideas, rather than from the evidence of a data evaluation, then you may licence the wrong source for your needs, or simply re-license from your incumbent despite better options being available.

The risks of basing your suppression strategy on such misconceptions, rather than evidence, could be significant - given the requirements of GDPR, organisations will not be able to base their compliance on assumptions which may lead to them holding inaccurate data. Failing to assess the performance of suppression as part of mandated data hygiene could risk incurring a significant financial penalty.

Under GDPR, data controllers are obliged to understand the products and services they use to maintain data accuracy and to take steps to ensure their solutions are compliant. Data evaluation during supplier selection as part of the suppression review process is therefore the golden key to compliance. It supports unbiased, evidence-based decision making and proof of a robust process.

"One of the UK's largest insurers recently evaluated the National Deceased Register suppression file and found its customer database contained in excess of 100,000 deceased Individuals on a database containing 22 million records"

Case Study

"One of the UK's largest insurers recently evaluated the National Deceased Register suppression file and found its customer database contained in excess of 100,000 deceased Individuals on a database containing 22 million records. This worryingly large number had gone undetected by all the suppression files it had previously relied upon for decades to keep its data up-to-date and clean."

5 Suppression, GDPR and beyond

Using suppression files to remove deceased records from a customer database will soon be a legal requirement. But it has long been best practice and a standard which any company that belongs to the Direct Marketing Association (DMA), for example, is expected to adhere to.

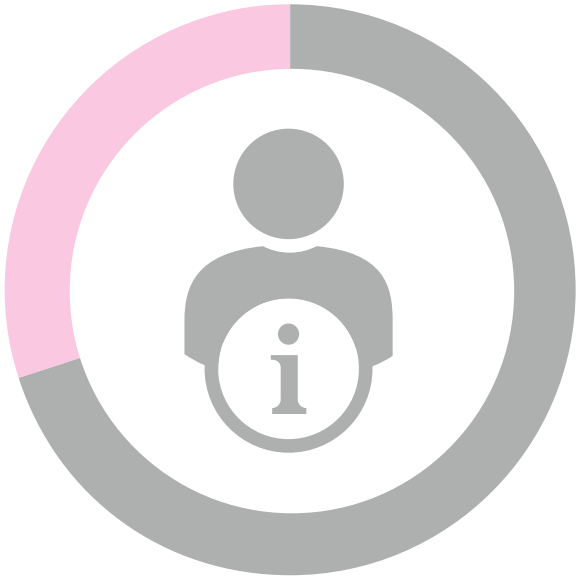
Consumers have an expectation that companies will do whatever it takes to ensure personal information is accurate and up-to-date. In research carried out by DataIQ, 70 per cent said they expect organisations to get personal details right every time. To the family or partner of somebody who recently died, receiving a communication in their name, whether by mail or email, is profoundly upsetting.

Just 20 per cent of consumers said they would tell some, but not all companies about a change in personal information in the same DataIQ research. And suppression provider Wilmington Millennium has found that, on average, consumers tell just five organisations when they move home - during the emotional turmoil following a death, this number is likely to be much lower. So it is clearly incumbent upon firms to adopt suppression to avoid causing distress.

Business benefits are also directly attributable to the use of suppression to clean up customer records and remove or flag deceaseds. Stealing items of mail which have been sent to a dead person or an empty property is common criminal practice and a first step in identity fraud, a crime to which one in seven people in the UK now fall victim at an annual cost of £3.3 billion, according to the National Fraud Indicator. Individual companies have to foot the bill for these frauds - avoiding them via suppression is a first line of defence.

GDPR is placing a new emphasis on maintaining customer data to the highest standard, with an in-built implication that screen out deceaseds is part of that requirement. It will not be the only piece of legislation to impose that obligation - if a business offers any sort of regulated service, from credit terms to product insurance or contractual agreements, then other laws covering anti-money laundering, knowing the customer or payment services come into play.

Suppression has a significant benefit to offer all types of marketers through improving campaign performance, reducing costs and protecting brand reputation. It is also now at the centre of legal compliance and customer engagement. With GDPR due to be enforced from 25th May 2018, the time to review and refresh your suppression strategy is now.



"70 per cent said they expect organisations to get personal details right every time"

About DataIQ

DataIQ aims to inspire and help professionals using data and analytics intelligently to drive business performance across their organisation and in every industry sector.

Specifically, DataIQ helps business professionals to understand the benefits of adopting data-driven strategies, develop compelling business cases, implement best practice, ensure they comply with data regulation, and understand how to use the latest tools and technology to deliver sustained business improvement.

DataIQ achieves this by providing essential insight, help and know-how from proprietary research, analysis, best practice and comment from industry leaders and data experts. All made easily available through high-quality events and digital channels.

Our unique community of business decision-makers and influencers - working across functions in FTSE 100, large and mid-market organisations - is growing rapidly as a consequence of this unique focus. Importantly, DataIQ provides the bridge for ambitious vendors, agencies and service providers to ifluence this hard-to-reach and unique community.

DataIQ is committed to championing the value of data-driven business and best practice through focusing on the success stories of data-driven professionals with initiatives including the DataIQ 100 and DataIQ Talent Awards, plus many other events and programmes. We contribute actively to trade and government bodies, including the DMA, IDM, PPA, techUK and UKTI.

For the latest information on how DataIQ can help your organisation go to www.dataiq.co.uk.

For information on how to become a commercial partner to DataIQ, call Adrian Gregory or Adam Candlish on +44 (0)20 3829 1112 or email adrian.gregory@dataiq.co.uk and adam.candlish@dataiq.co.uk

About The Ark

We are experienced industry professionals who passionately believe the foundation of any successful business depends on the quality of its databases and that the process starts with having clean, accurate and reliable data. Without this, every action and decision taken is potentially flawed.

For these reasons, The Ark launched the National Deceased Register in 2011 and Re-mover in 2013 having identified a need for truly reliable suppression data. Both files have now been universally acclaimed to be the most comprehensive accurate and reliable files available on the market.

To book an evaluation for your suppression services, contact The Ark today on 0370 334 1510 or email us 2by2@ark-data.co.uk

The Ark
Unit 1, The Old Barn
Wicklesham Lodge Farm
Faringdon
Oxfordshire
SN7 7PN