melissa

A **MELISSA** WHITEPAPER

Guide to Public Sector Contact Data Quality

How to reduce fraud, drive better outcomes, increase agility, and reduce back-office costs.

TABLE OF CONTENTS

DATA QUALITY: FROM PUBLIC SECTOR ORGANISATIONS TO CITIZENS

Data held by public sector organisations is one of their most valuable assets, so it's vital that it is fit for purpose. Successful processes to deliver data quality and new technology powering identity verification practices can improve your organisation and outcomes for your users by:

- Improving communication efforts
- Reducing costs
- Having a clearer view on strategic objectives
- Reducing fraudulent activity
- Staying compliant
- Driving revenue
- Gaining a deeper understanding of your users
- Bettering targeted budgets

This guide will provide a framework on how public sector organisations can put themselves on the path towards better quality contact data and maintain a clean and accurate citizen database throughout the whole data quality and know your citizen (KYC) lifecycle.

THE CURRENT STATE OF PUBLIC SECTOR DATA

We see a recurring issue amongst many public sector organisations holding stale and inaccurate contact data on their users or citizen database. The common approach to addressing such data quality issues is of lower priority for most, often being seen as a backroom task. It's something that may or may not be done, and only comes to a head when errors arise based on decisions made from one's current dataset[1].

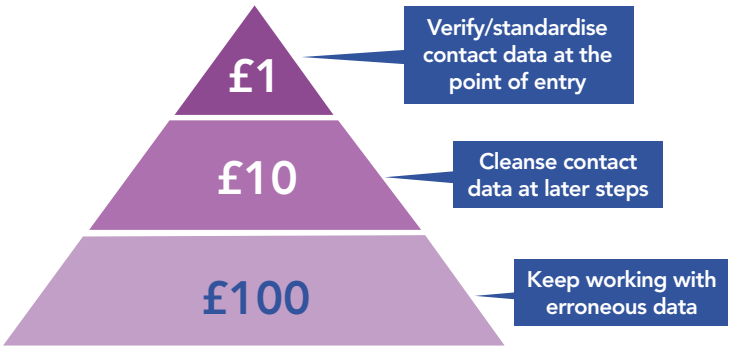
The historical approach in this sector (like many others) has been of tolerance to this problem and finding workarounds for poor quality contact data is common.

Another factor to consider is that many organisations in this space have multiple departments to deal with. With their historical ways of processing and managing incoming data, this leads to a lot of contradictory approaches and a lack of consistency across all departments.

The extent of these difficulties leads to data quality perhaps being poorly understood, and that work on data quality can be reactive, rather than evidence based. It can often be treated as a quick fix rather than curing the actual cause, leading to ineffective improvements, and wasted resources.

Businesses working within the public sector must recognise that a customer database goes stale at an average rate of 2% each month, rolling up to 25%, or 1 in 4 of every citizen's record per year. This is due to people moving home, changing emails, phone numbers, changing jobs, marrying, dying, and divorcing etc, etc.

CONSIDER THE 1 -10 - 100 RULE WHICH STATES:



It can cost an average of **£1** per record to verify at the point of entry, with correct data quality and know your citizen processes in place.

It costs an average of **£10** per record if existing records are cleansed intermittently to correct, update and deduplicate records in batch.

It costs an average of **£100** per record if nothing is done to fix bad data quality – reflecting wasted communication efforts, materials, a poor reputation, and a 'bad' outcome for citizens with data having to be retrospectively corrected by the public sector organisation.

THE MODERN ERA

Access to public sector services has always been a top priory for many citizens even before the ongoing challenges of the pandemic. This has put huge amounts of pressure on public sector bodies and government agencies to keep up with such demand during challenging times financially. The push to improve digital engagement with citizens leaves a lot of organisations in this space struggling to hold up to date records on individuals and in turn more open to fraudulent activity.

Fraud was already a big issue with the National Fraud Authority (NFA) estimating that around £40 billion was lost annually in the UK, and this is set to increase as we continue to move forward with a more 'digital first' approach[2]. This creates the perfect storm of loss to the taxpayer, reputational risk to the organisation, and undermining trust in the government due in part because of bad data quality.

Statistics show that public sector organisations trail behind the private sector in implementation of such software and processes to combat fraud and ensure accurate contact data[3]. Organisations within the public sector must be aware of the below points if they want to maintain the trust of their citizens who rely on their services and put themselves at the forefront on the fight against fraud.

1. Clean communication

Ensuring clean and accurate contact data on a citizen database will improve your communication efforts, save costs on wasted postage / deliveries, and allow you to build stronger relationships with the public through various communication channels: post, email, web chat, and phone.

2. Fraud can start with bad data quality

It can be as simple as a person creating a fake address, email, and phone number to claim benefits, which is why robust data quality and identity verification practises should be implemented.

3. There is no 'standard' solution

Different departments, partner agencies, councils, and organisations in the public sector will have their own challenges which is why there is no one size fits all approach to data quality and identity verification. However, customisable technologies (that already exist) can be tailored to fit specific use cases. Holistic responses to issues relating to poor data quality and risk of fraud are key, rather than just a hopeful quick fix.

4. Remote engagement through a more digital approach

Being more digital focused means a greater possibility of fraudulent activity. This requires organisations to be agile and adapt their approach to deal with the evolving risk landscape.

5. Accuracy from the start

Preventing inaccurate contact data from entering your organisation's systems and preventing fraud through effective and robust processes, reduces financial loss and reputational damage. It's important to note it requires fewer resources than an approach focused on detection and recovery.

[1] HTTPS://PWC.BLOGS.COM/FILES/FRAUD-IN-THE-PUBLIC-SECTOR_FINAL.PDF

[2] HTTPS://ASSETS.PUBLISHING.SERVICE.GOV.UK/GOVERNMENT/UPLOADS/SYSTEM/UPLOADS/ATTACHMENT_DATA/FILE/778306/GUIDETOMANAGINGFRAUDFORPUBLICBODIES.PDF

GETTING THE BASICS RIGHT

While obtaining the right address, email and phone details of individuals seems straightforward, we see a lot of organisations getting this wrong. Not having the right processes in place to ensure addresses entered are verified postal addresses, emails are pinged in real-time to ensure they can receive mail and phone numbers are live and callable, is a big issue.

With data, such as an email address, phone number, and postal address, organisations can verify more information about an individual and create a thorough customer record. Administrators with the right tools can confirm an identity, amend addresses, confirm proof of address, and residency status.

It's vital to take this a step further to verify an individual's entire record. The escalation in data breaches has led to an increased number of criminals posing as a legitimate person.

This means matching a particular name to an accurate physical address, email address, and phone number to trusted sources reference data, such as electoral roll, credit agency and utility company, at the touchpoint and in real-time. This is very important to suppress fraud. It's this easy approach that will give public sector organisations more confidence that persons engaging with their services are who they say they are.

IT STARTS WITH ADDRESS

In both public and private sectors, the principle of "know your customer" (KYC) or "know your citizen" is fundamental to reducing the risk of fraud and maintaining trust. Address verification plays a crucial role in this process by confirming that individuals provide authentic and accurate addresses and that they actually reside at those locations. This verification is not merely a procedural formality but a critical step in ensuring the integrity of various services and transactions.

When addresses are not verified, organisations face several potential pitfalls. For financial institutions, failure to verify addresses can limit the availability of payment options. This might mean customers cannot complete transactions, leading to lost business and customer dissatisfaction. In sectors such as insurance, unverified addresses can lead to unsuccessful onboarding, where new customers are unable to set up accounts or access services, again resulting in lost opportunities and revenue.

Moreover, in the realm of claims processing, particularly in insurance and social services, unverified addresses can result in denied claims. Without accurate address information, organisations cannot validate the authenticity of claims, leading to mistrust and dissatisfaction among legitimate claimants. This can also open the door for fraudulent claims, as criminals exploit weaknesses in the verification process.

A SINGLE CITIZEN VIEW

Gaining a single citizen view (SCV), or a 360-degree view, is highly beneficial for public sector organisations as it consolidates all interactions and data related to a citizen into a unified record. This comprehensive perspective enhances service delivery by enabling personalised services and streamlined interactions, ensuring citizens receive consistent and accurate information across various departments. It improves operational efficiency by simplifying administrative processes and saving time, allowing public sector employees to quickly access complete and accurate citizen information, thereby speeding up service delivery and issue resolution.

Data deduplication plays a crucial role in achieving a SCV by identifying and removing duplicate records, consolidating data from various sources, and cleansing data to correct errors and inconsistencies. This process eliminates redundancy, ensuring that each citizen is represented by a single, accurate record, and prevents data fragmentation. Furthermore, it standardises data formats and entries, making it easier to integrate and compare information from different systems.

Data deduplication also ensures the accuracy of information through validation processes such as address, name, phone and email checks, and by continuously monitoring for duplicates or inaccuracies. By enhancing system interoperability and supporting interdepartmental collaboration, it creates a cohesive and comprehensive view of citizen data accessible to authorised personnel. This integration facilitates smoother data exchange and coordination across different departments, ensuring that public sector organisations can better meet citizen needs and that services are delivered effectively and efficiently.

IDENTITY VERIFICATION & KYC INITIATIVES

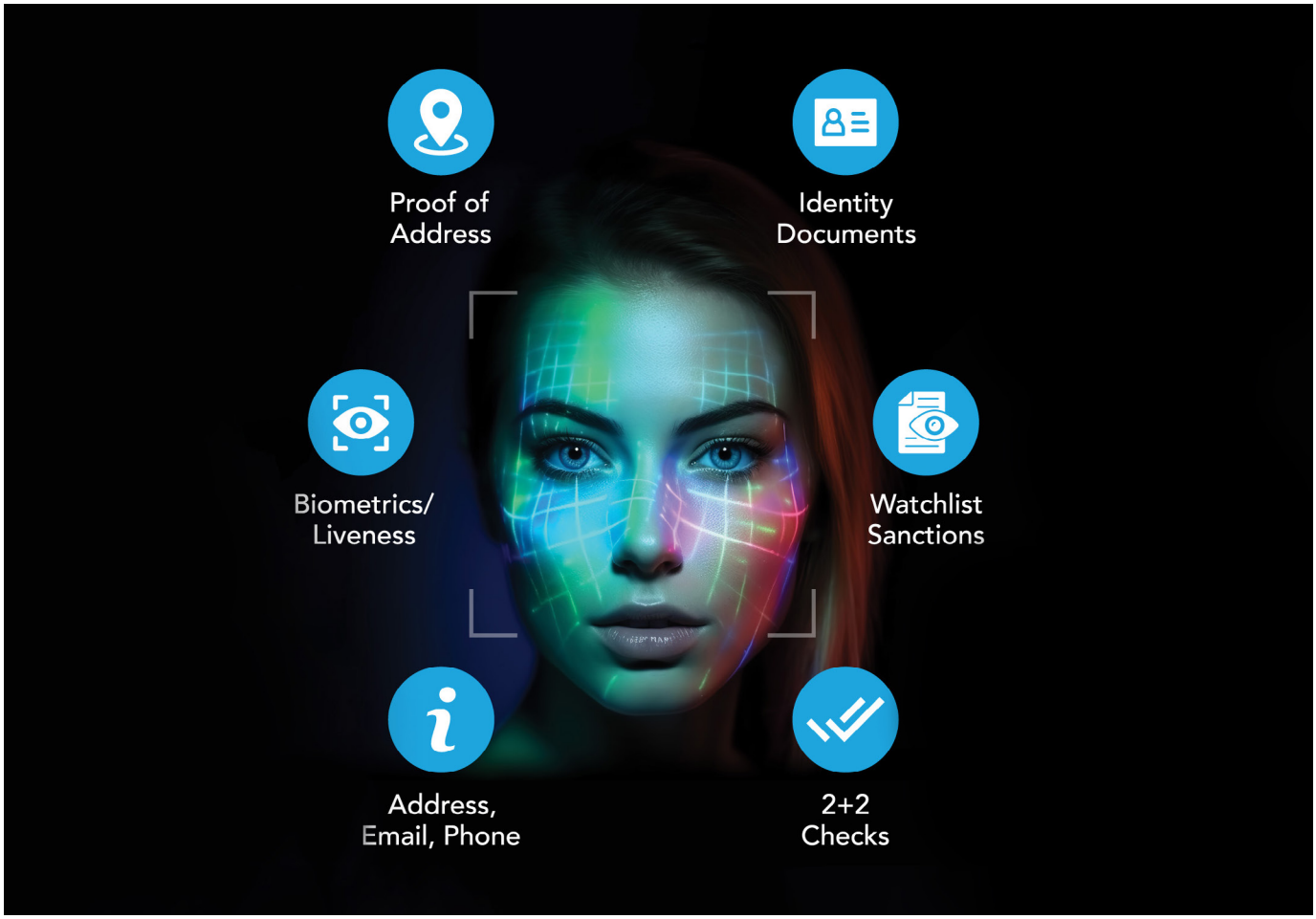
A layered approach is the answer

Fraud poses a significant challenge for organisations across all industries, but it's especially critical to address within the public sector due to the substantial flow of funds involved. Protecting taxpayer money from fraud is essential for ensuring that communities receive the maximum value from their taxes. This issue isn't unique to the UK; globally, there has been an uptick in reported fraud cases, largely fuelled by the digital revolution.

Understanding the extent of the problem is crucial for developing effective countermeasures. Government estimates suggest that fraud and error loss in public expenditure and income ranges from 2.1% to 3.8% annually. Similarly, improper payments in the United States account for 5.1% of expenditure, while EU estimates range from 2.2% to 3.8%. These figures represent significant opportunities to stretch taxpayers' money for greater impact [4 5].

One powerful tool in combating fraud is electronic ID verification (eIDV). This technology employs a layered approach to authenticate users during onboarding processes, ensuring a smooth and secure experience. It begins by verifying initial contact details such as addresses, phone numbers, and emails, and then proceeds to establish residential status and proof of address through methods like a 2+2 check.

Additional layers, including age verification and screening against politically exposed persons (PEP) lists and global watchlists can be added to enhance security further. Moreover, eIDV enriches customer records by identifying inaccuracies and adding missing data, improving data quality and integrity.



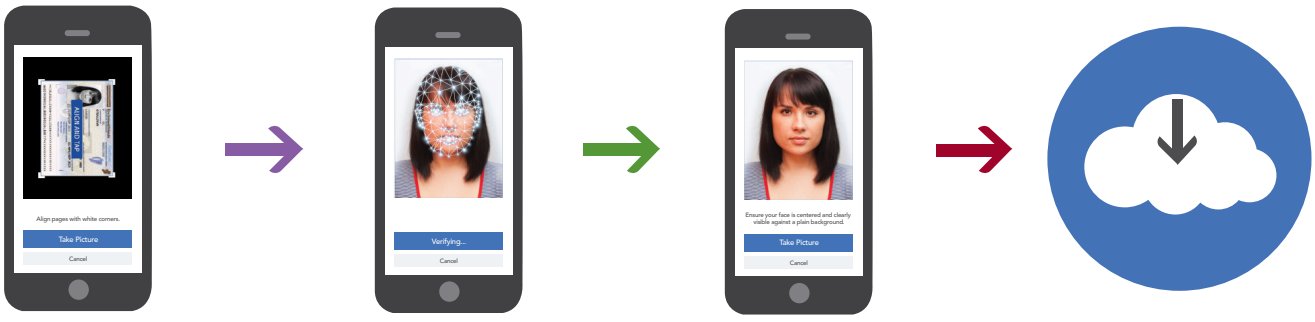
ID DOCUMENT VERIFICATION TO DETERMINE AUTHENTICITY

Additionally, to make 'live onboarding' work, public bodies need the technology to determine authenticity. This means scanning copies of people's ID documents, such as driver's licenses, passports, and utility bills. These can then be held on file and stored for customer due diligence. By using optical character recognition (OCR) and machine-readable-zone (MRZ) technology, it's possible, in real time, to determine whether the ID document is real and valid – eliminating the time taken in manual processing and the potential for human error. Furthermore, the photo ID embedded in these scanned documents supports biometric ID verification, such as facial recognition, which in turn can be used to match against a person's real-time photo or "selfie" taken from a mobile device. Motion sensors will also determine the 'live status' of the candidate presenting themselves. This helps those in the public sector to securely speed up engagement with customers and eliminate time consuming and resource wasting "manual method" checks.

ARTIFICIAL INTELLIGENCE (AI) NOW A VITAL ROLE IN IDENTITY VERIFICATION

The use of AI is set to make a big shift in the ID space, playing an increasingly important role in delivering automated KYC and AML compliance, both in user onboarding and retrospective ID investigation. One form of AI, semantic technology, associates words with meanings and recognises the relationship between them. The machine reasoning and automated pattern recognition provided by this technology can help to identify possible fraudulent applications in real time. Also, semantic technology makes it possible to apply context and make inferences with data, ensuring properly validated identities as well as broader data quality and integrity.

As the number of AML and KYC regulations proliferate, ID investigation cannot be avoided if compliance is to be achieved. Speed, efficiency, and cost are the key reasons public bodies should leverage existing technology such as eIDV, document scanning and biometric verification, to launch an automated 'live onboarding' process behind the scenes. It's also technology that can be successfully used to ensure AML and KYC compliance.



KYB IN TANDEM WITH KYC CHECKS

In today's digital age, it's crucial that eIDV platforms utilised by public sector organisations offer comprehensive Know Your Business (KYB) checks. These checks are essential for fully understanding the risks posed by both new and existing suppliers, business customers, and partners. Fraudsters often exploit shell companies or umbrella structures that lack substance, making KYB verification indispensable in combating such fraudulent activities. By validating organisations through KYB processes, the potential for financial crimes such as money laundering and terrorist financing can be significantly diminished, thereby mitigating the risk of reputational damage and financial losses.

We consider KYB checks to be an obligatory tool for the public sector, playing a pivotal role in upholding regulatory compliance, preventing financial crimes, managing risks, promoting transparency, and maintaining integrity in business transactions. The combination of KYB and KYC processes working in tandem not only safeguards public funds but also heightens accountability and fosters trust and confidence among citizens.

[4] HTTPS://WWW.MELISSA.COM/UK/RESOURCES/WHITEPAPERS/PDF/WP-KNOW-YOUR-CITIZENS.PDF

[5] HTTPS://WWW.WIRED-GOV.NET/WG/CONTENT.NSF/INDUSTRYNEWS/HOW+TO+TACKLE+FRAUD+IN+A+GLOBALISED+WORLD

SUPPRESSION TECHNIQUES

Stats show that within a year, 7 million individuals move home in the UK, 600,000 people pass away, and a significant number of individuals opt out of mailing and telephone communication channels (MPS/TPS) from businesses[6].

A key part of maintaining the quality of consumer data you hold is the identification of citizen who may have opted out of direct marketing, moved, gone away (not provided a forwarding address) or sadly died. This ensures that customer and prospect data is compliant with GDPR standards and is the benchmark for responsible data management and communication. Consumers expect it, the law requires it, and it delivers massive savings for better ROI, while reducing the risk of brand damage.

Goneaways: Mailing to goneaways at their old address is an obvious waste of budget, which is why suppressing your database against Royal Mail's National Change of Address File (NCOA) and a wide list of utility files will flag and update all changes of addresses in the UK, something that can also be achieved in many territories.

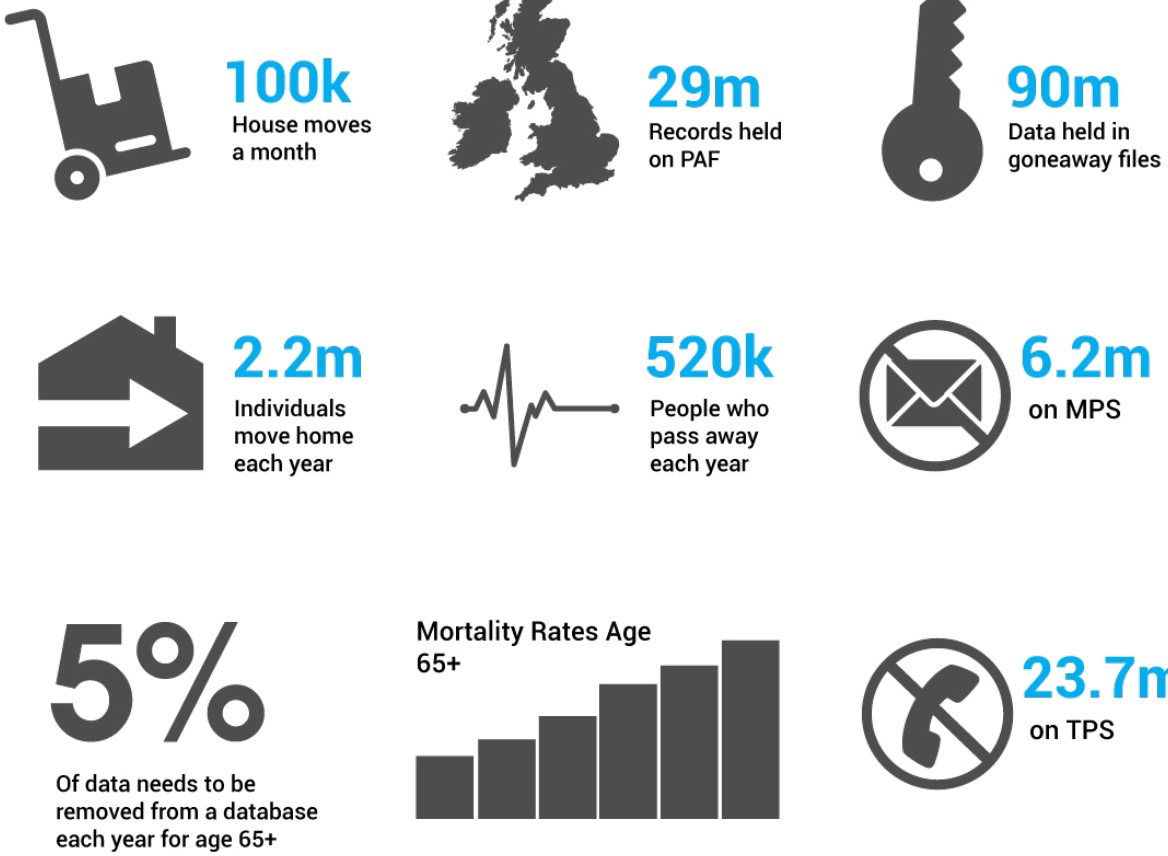
Deceased: Holding records of deceased individuals incurs penalties, breaches DPA & GPDR compliance, and opens the potential for deceased identity fraud and theft, not to mention being a possible area for brand damage. Regularly screening your database against The Bereavement Register (TBR) to remove decreased records should be compulsory. It's the most accurate and reliable deceased suppression file updated monthly.

Mailing/Telephone Preference Service (TPS / MPS): These play an important role for public sector organisations in helping to recognise persons who have opted out of direct communication from telephone and mailings. It's vital in maintaining GDPR compliance and not wasting budget and time with individuals who don't want to see your messages.

The following occurrence is based on real campaign metrics:

- Client A has a database of 2 million records selected for an acquisition mailing campaign
- Suppression flagging using utilities & the NCOA file identified 10% of the individuals in the database had changed address
- Another 10% were identified as opted out of TPS/MPS communication
- 5% were flagged as deceased
- That's 100k individuals flagged and suppressed as goneaways
- Based on their mailing pack price of £0.50 removing those goneaways saved £50,000
- An additional 10% opted out of communication which saved an additional £50,000 (not including costs in resources for telephone communication)
- A further 5% was flagged as deceased adding another £25,000 in savings

After undertaking a full suppression cleanse on their database they were able to save £125,000, keep in touch with moving customers and maintain compliance.



DATA ENRICHMENT

Achieving a clean and accurate database is just the first step. The next crucial phase involves enriching it with valuable insights about current users. While data enrichment is not as widely undertaken, there is a significant opportunity for public sector agencies to enhance their operations by adopting this technology. It's important to note that strict adherence to data privacy rules is paramount, which can be ensured by partnering with reputable providers.

Adding additional elements to existing data provides valuable insights into individual interests and demographics. For instance, details like whether homeowners have children or businesses' average sales volume can greatly influence interaction strategies. This insight enables public sector organisations to tailor messaging and engagement methods effectively, ensuring they connect with their audiences in the most impactful ways.

1. Improved Decision-Making:

By enhancing existing data with demographic, socio-economic, and geographic information, public sector organisations gain deeper insights, enabling more informed decision-making and policy formulation.

2. Enhanced Service Delivery:

Enriched data enables better understanding of citizen needs and preferences, facilitating more targeted service delivery and support allocation.

3. Resource Allocation Optimisation:

By identifying areas with the greatest need for services and resources, governments can allocate resources more efficiently, maximising impact and benefit.

4. Predictive Analytics:

Enriched data allows governments to leverage predictive analytics, anticipating trends and planning proactively to address emerging challenges.

5. Fraud Detection and Prevention:

Enriched data aids in identifying patterns indicative of fraudulent activities, empowering governments to detect and prevent fraud more effectively.

6. Improved Citizen Engagement:

Enriched data enables personalised communications and engagement efforts, enhancing citizen engagement and participation.

7. Data-Driven Policy Evaluation:

Enriched data facilitates rigorous evaluation of policies and programs, enabling evidence-based decision-making and continuous improvement.

EASE OF CONNECTIVITY

Many public sector organisations use database management systems like Microsoft SQL Server, Salesforce, or MS Dynamics. These technologies facilitate seamless access to third-party applications by acting as connectors between systems and operating at high speeds. Tools can be accessed easily without further integration—just drag, drop, and start using.

These prominent database management systems provide organisations with direct access to data quality capabilities, allowing them to clean and verify contact data. There's no need to outsource or navigate complex data privacy and compliance issues, as data remains secure behind the organisation's firewall, eliminating the risk of data breaches.

By sourcing the right data quality components, public sector organisations can collect data from any source and use it to cleanse and transform their databases. This enables them to gain immediate insights for actionable intelligence.

It's best to select a data quality provider that offers a comprehensive suite of easy-to-integrate solutions for all popular data management systems. This suite should include tools for cleansing data to correct inconsistencies and validating data using powerful global address, name, phone, and email verification processes. Additionally, it should have a component for matching data, utilising advanced fuzzy matching algorithms to eliminate duplicates.

Furthermore, the ideal data quality suite should be adaptable and scalable to meet the evolving needs of public sector organisations. This includes the ability to handle large volumes of data and integrate seamlessly with existing IT infrastructure. The flexibility to customise data quality processes to specific requirements is also important, ensuring that the solution aligns with the organisation's operational workflows and compliance mandates.

THE RESULTS OF DATA QUALITY & IDENTITY VERIFICATION

Implementing data quality and identity verification processes in public sector agencies not only boosts service delivery but also transforms their approach to data-driven governance. It's advisable for public sector entities to adopt a pragmatic approach, starting with small projects to identify issues and areas of data inaccuracies and focusing on data management projects with the most significant impact, initially providing a baseline for addressing further issues.

A basic approach demonstrates that even small investments can yield meaningful changes, potentially leading to increased budget and resources for larger projects in the future. The more accurate the data, the better the insight and operational efficiency.

The benefits of contact data quality and identity verification for public sector organisations in the UK are extensive:

1. Enhanced Service Delivery:

Accurate information about citizens enables personalised and efficient service delivery, improving citizen satisfaction and outcomes.

2. Fraud Prevention:

Identity verification reduces the risk of identity theft and fraudulent claims, safeguarding public funds and maintaining trust in government services.

3. Data Security and Privacy:

Ensuring the accuracy of contact data and verifying identities enhances data security and privacy, protecting citizen information from breaches or misuse.

4. Compliance with Regulations:

Identity verification ensures compliance with GDPR and AML requirements, reducing the risk of penalties or legal action.

5. Efficient Resource Allocation:

Accurate data enables effective resource allocation, maximising the impact of public spending and improving overall efficiency.

6. Improved Decision-Making:

High-quality data provides valuable insights for informed decision-making and policy formulation.

7. Enhanced Public Trust and Confidence:

Maintaining data quality and identity verification processes fosters trust and confidence in government services, leading to stronger relationships and increased cooperation.

In conclusion, contact data quality and identity verification are essential for UK public sector organisations to deliver efficient, effective, and trusted services while ensuring regulatory compliance and protecting public funds and data.

SOLUTION CHECKLIST

What to consider when choosing identity verification & data quality software

- [ ] Easy integration
- [ ] Low code / No Integration / Out of the Box
- [ ] Availability as a web service (cloud) interface or a locally installable on-premise API
- [ ] Optional real-time and batch processing
- [ ] Detailed and meaningful result codes from which subsequent business logic can be built
- [ ] Real-time data validation is done quickly (within milliseconds)
- [ ] Can be streamlined with a structured framework to serve policies across different departments
- [ ] Automatic & regular updating of reference data (no impact on service delivery)
- [ ] Best of breed UK & international country coverage
- [ ] Scalable, flexible & customisable to support all types of organisational needs, big or small
- [ ] Free customer support in local time & language, with 24-hour support available for out of hours
- [ ] Dedicated contact person for support & service-oriented customer care
- [ ] Compatible with any application (e.g., Microsoft SQL, Salesforce, etc.)
- [ ] Transliteration of foreign fonts
- [ ] Free proof-of-concept (PoC)
- [ ] Non-binding & free tests for independent evaluation on test environment
- [ ] Compliance with GDPR & other data protection guidelines including security certifications


melissa

melissa

www.melissa.com/uk

Speak to a Specialist

About Melissa

Our almost 40 years of address expertise started with ZIP+4 and turned into so much more. Melissa is a single-source vendor of global address management, data quality and identity verification solutions that help organisations harness accurate data for a more compelling customer view. Our industry-leading solutions have processed over 1 trillion address, name, phone and email records, making it clear why thousands of businesses worldwide trust Melissa with their data quality needs. For more information, visit www.melissa.com/uk or call +44 (0)20 7718 0070.

UK

Floor 37, 1 Canada Square
Canary Wharf, London
E14 5AA, United Kingdom

+44 (0)20 7718 0070 I Info.uk@melissa.com