Data Protection Impact Assessment

Date of approval and issue	March 2021
Document version	v2.0
Changes from previous version	Updated Identification of Risks and Mitigation
Approved by	Demography & Policy Analysis Manager
Review date	March 2022
Senior owner	Demography & Policy Analysis Manager
Document owner	Head of Strategic Crime Team

Contents

1. Requirement for a DPIA

SafeStats is a project within the Greater London Authority (GLA), which centrally collates record-level datasets from a variety of sources, relating to crime, disorder and safety incidents, before making them securely available to authorised users via a web-based portal. SafeStats also contains the personal details of users, as provided upon system sign-up.

The key processing involved is to standardise the received datasets to make them comparable with one another, so that web application functionality can 'read across' common fields within datasets relating to the time/date/location and type of incident.

No datasets held by the GLA in SafeStats contain directly personally-identifiable information, due to either the limited information recorded/provided (e.g. the date/time, station details and type of offence recorded by the British Transport Police) or have undergone a process of pseudonymisation (e.g. the spatial suppression of dispatch location provided by the London Ambulance Service).

Due, however, to the common categories of information within the datasets hosted within SafeStats, and their subsequent ability to be cross-referenced, the data, when considered as a whole, should technically be considered as potentially 'containing data that may indirectly identify an individual'. Under Article 4(1) and Recital 26 of GDPR and DPA 2018 all data is therefore considered as personal.

With this in mind, and the relevance to 'matching/combining datasets', as set out in Article 29 working party of EU data protection authorities (WP29), a DPIA is required as the SafeStats processing carried out by the GLA is of a type *likely* to result in a high risk/harm to an individual if identified.

It should be noted, however, that the potential for identification of individuals is significantly limited at the GLA processing stage as the data:

- is already very limited at source,
- is securely stored,
- is only accessible by a small number of highly trained and authorised GLA staff, and
- could only *potentially* be used to identify an individual under *very* specific circumstances, through reliance upon additional information obtained from other data sources external to SafeStats.

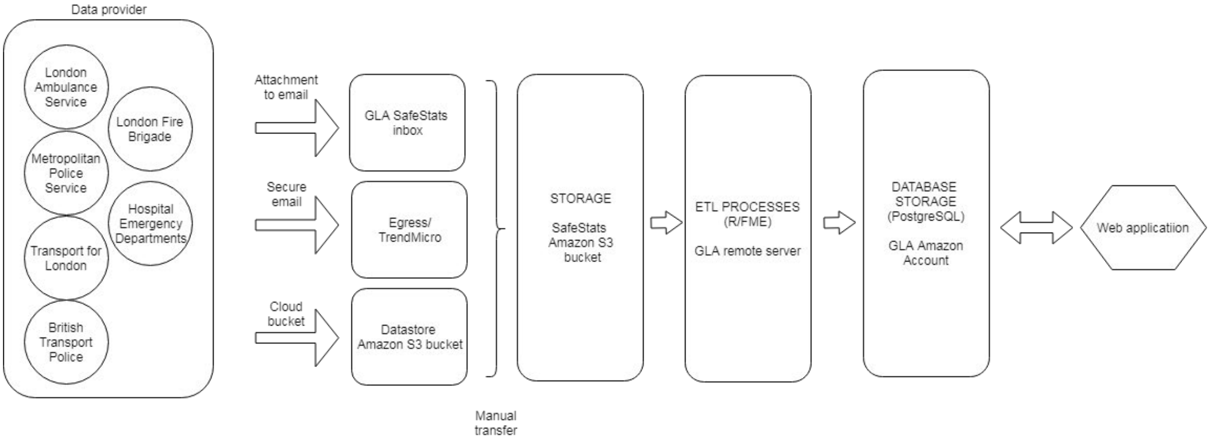
It must also be considered that *even* in a 'worst-case scenario', where all the data available on SafeStats concerning either a specific individual or incident is combined, the collective information would *not* be greater than could be derived from an eyewitness account or a media report.

This DPIA specifically relates to the GLA's responsibilities as both a Data Controller and the initial processor of the datasets and has not been written for 'end-users' (organisations) who may download data from the SafeStats website. These organisations, in also becoming Data Controllers for the SafeStats data, would be recommended to complete their own assessment about how any data matching they undertake could render an individual data subject more identifiable, including their own considerations on their position on Article 14.

This DPIA aims to assess the risks to the fundamental rights and freedoms of the data subjects stemming from the collection, collation and storage of personal information within SafeStats.

2. Processing of data

2.1 Nature of processing



Datasets are received from a variety of data providers from their own internal systems, with minimum agreed schemas set out in the individual Data Sharing Agreements. SafeStats determines that the data provided meets minimum requirements for analysis and is not excessive to its purpose.

The data is provided through a method mutually agreed with the data provider, either via:

- A flat file appended to an email and sent to a secure GLA email account only accessible by SafeStats staff members[1],
- A flat file upload to a secure web mail account (e.g. Egress/Trend Micro) only accessible by the data provider and SafeStats staff members, or
- A flat file upload to a designated cloud bucket (e.g. Amazon S3) only accessible by the data provider and SafeStats staff members.

It is accepted that any data transfers that involve steps additional to a data provider directly inputting their data into the end-stage database of the GLA may reduce the level of risk held by the GLA. However, from a host data security perspective it is not feasible for data providers to have this level of access. Risks have been minimised elsewhere by utilising only a single additional transfer step, using methods that are agreeable to both sides of the transfer, and with the fewest individuals involved/having access to the transfer.

In the first two of the three transfer methods, the data is then manually moved/saved to the secure SafeStats Amazon S3 bucket which is located inside the GLA VPN. This bucket is only accessible to SafeStats staff members and the GLA's Technology Group from an administrative position. Data files are then removed from the original sources. Any data provided prior to 6 months of the current date is also removed from the SafeStats S3 bucket.

[1] *GLA Technology Group staff have overall administration-level access to these locations, with any access recorded and auditable in-line with established GLA policies and procedures*

There may also be instances of SafeStats staff members retrieving data directly from an organisation's website either through a manual extraction/download of the required data or through the API associated with that website. These datasets will also be moved/saved to the SafeStats Amazon S3 bucket.

All data is read from the SafeStats S3 bucket into ETL software located on a GLA Azure server with limited access. Here the data is checked, reformatted, geocoded and categorised. No data is however stored on this server.

Once processed, data is written out to a PostgreSQL database on an Amazon instance within the GLA VPN where it is appended to historic data. Access to this instance is limited to SafeStats staff members. The GLA Technology Group staff have overall administration-level access to these locations, with any access recorded and auditable in-line with established GLA policies and procedures.

The private SafeStats web application reads the data directly from the PostgreSQL database, making the agreed datasets available to authorised users to access, download and utilise in their home organisations.

The risk of incorrectly receiving high-risk de-anonymised data is low through the agreement of datasets to be shared in the DSAs and the strict quality assurance of data by data providers before being sent. SafeStats also have automated data processing checks in place to ensure that the content of the data is correct and within "expected ranges"; meaning that any additional data fields/columns are identified from the onset. However, if unplanned data is received in the form of additional fields of data, or disclosive content in an existing field, these will be identified through the initial ETL QA process outlined above. In these circumstances, the data provider will be immediately notified, and a replacement dataset sought, with the original deleted. The GLA retention policy regarding emails is that the email is then available for 30 days if recovery is required before being permanently deleted under email provider policy.

2.2 Scope of processing

Data collected for SafeStats is in record-level format where one row of data relates to one record. Depending on the data provider, these records can relate to a criminal offence, an emergency vehicle dispatch, or a reported safety-related incident. As noted previously, if matched with other datasets under certain circumstances, this may result in the identification of an individual. Whilst this risk is low, it is accepted that this would cause distress or damage to that individual.

The general structure of the datasets include temporal, spatial and categorical information about the record. One of the datasets provided to SafeStats contains special categories of data as per Article 9(1) of the GDPR; while criminal offence data is kept to the minimum of the category and subcategory of the offence.

All data released by data providers has been granted suitable for sharing via SafeStats mainly through their suppression of spatial location data to a de-identifiable level.

Data is collected on a monthly basis, covering either the most recently completed full month of records, or a wider period of 24 months or greater to account for historic changes. Once processed, the data is held in the secure GLA database for the web application to source. Source data is only held for 6 months after the date of receipt once uploaded to the database, to cater for potential technological issues.

From a wider data retention perspective, a key purpose of SafeStats is to allow the scanning of trends of data over long periods of time. It is therefore important that a wide range of data is available to end-users. Whilst data is held in some circumstances as far back as 2001, SafeStats' policy to balance purpose-relevance (based on user feedback) and data retention is to make only the most recent 10 years of data available to end-users. Data prior to that is stored securely and separately by SafeStats and available on request. The user requirement for data prior to the most recent 10 years will be reassessed on an annual basis.

The data for most of the data providers, covers records located within the GLA boundary. Approximately 265,000 records are added across all datasets each month, which is a rough approximation to the number of persons that these records affect.

Although, it is accepted that a data breach *could* occur from the data-sharing under the SafeStats project, the risk is deemed to be low and mitigated by:

- The processing pathways utilised in this project sitting within industry standard GLA security architecture,
- We have had full penetration-tested by an independent agency,
- Whilst user error is a possibility, data process automation has been implemented wherever possible, alongside staff training,
- SafeStats staff are aware of their responsibilities under the GLA Breach policy as well as corporate and personal responsibilities set out under the provisions of the GDPR.

2.3 Context of processing

Whilst there is no direct relationship between SafeStats/GLA and the data subjects referred to within the records collected, it is possible that in certain circumstances their data was not directly obtained from them by the data providing organisation ('Invisible processing'). An example being the age and gender of an injured party recorded in a call from a witness to the London Ambulance Service, without the permission of the injured party.

Article 14 of GDPR sets out the information that must be provided to an individual by the GLA about the processing of their data when collected under these circumstances; however, paragraph 5(b) states that these requirements do not apply where:

> *the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.*

An exemption to access rights requests also exists in Schedule 2, Part 6, paragraph 27 of the 2018 Act.

The GLA acknowledge that under the DPA 2018, the SafeStats data subjects have several rights that they can exercise in relation to the data that we are processing about them. We are mindful that under certain circumstances, by law, the data subjects have a right to, request access to their personal information, request rectification of the personal information held about them, and/or request erasure of their personal information.

For the SafeStats website users, the SafeStats team can easily and efficiently service these data subject rights requests. However, for the data subjects contained within the hosted datasets on SafeStats, there is insufficient data held within the datasets to directly identify the data subjects. The data held by the GLA for SafeStats is not intended to be identifiable nor does it include any direct identifiers. The GLA is provided this data by third party stakeholders who remove the direct identifiers before transfer. In order to be suitably satisfied of the identity of anyone wishing to exercise these data subject rights, that individual would have to provide SafeStats with considerably more data about themselves and the incident that involved them than SafeStats currently holds about them.

Due to the disproportionate effort involved in the GLA enforcing the latter type of these data subject rights, requests will *only* be facilitated where information is provided to reidentify the data subject; including the provision of the date, time and location of the incident. Although, the GLA accepts that this could potentially pose some minor difficulties to the data subject in effectively being able to exercise their own rights, should this additional information not be provided to the GLA then the SafeStats team will be unable to facilitate the request. The relevant rights request will then have to be re-directed by the data subject to the organisation from which the data originates.

To ensure compliance with fairness and transparency, SafeStats has two publicly available fair processing notices (privacy policies) on its website; one to cover the data collected from SafeStats website users, and the other to cover the information provided by data providers to SafeStats. These fair processing notices explain what data is collected by the GLA, how the data is handled, the legal basis for processing, and how the information/personal data collected is protected. Due to the need to re-identify the data subjects, the GLA is not required to directly provide the fair processing notice to the data subjects contained within the information received from the SafeStats data providers. As referred to in relation to data subject rights requests, whilst this is self-evidently not impossible, it is likely to represent a disproportionate effort on the part of the GLA given the aims and objectives of the processing, the fact that the personal data was obtained from a source other than the data subject, and that the identification of the data subject is never the intention.

2.4 Purpose of processing

The purpose of the processing is to make the data available in the most efficient format to authorised SafeStats users in public authorities who have a role in community safety and reducing crime. Using this pre-formatted, cleansed and comparable data, users are then able to spend more time conducting research and analysis of the data to identify trends and patterns and make recommendations for related tactical and strategic action within their organisations. This has the intended benefit of reducing crime, improving levels of personal safety, and reducing the fear of crime.

The data from SafeStats is used by end-user organisations in a variety of different ways, including:

- Trend analysis to support strategic decision making as part of Local Authority Strategic Assessments,
- Data support to the Mayors' public health approach to violent crime, in particularly the work of the Violence Reduction Unit,

- Contextual insight to problem-profiles on a local and regional level,
- Bespoke 'underreporting' insight for knife crime profiles through ambulance and hospital data, as part of the MOPAC information Sharing to Tackle Violence (ISTV) program, resulting in tangible benefit in policing operations,
- Support for the Mayor's priorities around crime and public safety, health and the economy including keeping children and young people safe, tackling violence among women and girls, and fighting knife crime.

3. Consultation process

Article 35(9) provides that, "where appropriate", organisations should seek "the views of individuals or their representatives". However, as SafeStats has no direct relationships with individuals and has insufficient data to fully identify the data subjects contained within the data being shared with them, it is not possible to consult directly with these data subjects.

Therefore, as part of the ICO Sandbox work, the SafeStats team commissioned external research to explore the public attitudes to data sharing for the purposes of violence reduction. The research focused specifically on those who were most likely to be impacted upon by violent crime, either as a victim or a perpetrator. This enabled the SafeStats team to demonstrate an appropriate level of care and respect for the rights of the data subjects, whose data we will be receiving and processing; while providing an insight in the areas of data protection that they have the most concerns about.

The views articulated by the research subjects included both a positive view of data sharing for the purposes of violence reduction and support for the sharing of personally-identifiable data to help provide tailored crime diversion support for individuals; with their support for data sharing being very much based on that which is undertaken for benevolent intent only. This manifested in support for the processing of data relating to health and education but did not extend to the processing of biometric data and physical location geotagging data, especially when undertaken by technological corporations.

Additionally, consultation with data providers and the SafeStats steering group will form part of the regular Information Sharing review process; where their views on this aspect of data sharing will be a standard agenda item. Up until this point, no concerns have been raised by data providers or the Steering Group members.

The authorising contacts at end-user organisations have been made aware of the potential of data matching, the prohibited use of it, and the potential requirement for a DPIA. Their views will be regularly sought on the process.

Relevant Information Governance, Technical, and Data Provider contacts have also been fully sighted on this issue, with an open feedback channel always available.

4. Necessity and Proportionality

The lawful basis for sharing the information (and therefore the processing of that information) is grounded in:

- Section 17 of the Crime and Disorder Act 1998 that requires the London boroughs to exercise their various functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that it reasonably can to prevent:

  - crime and disorder in their area (including anti-social and other behaviour adversely affecting the local environment);
  - the misuse of drugs, alcohol and other substances in their area; and
  - re-offending in their area,
- Section 115 of the Crime and Disorder Act 1998 that provides an 'express' gateway, which legally justifies the sharing of information where it is necessary to prevent crime and disorder or for crime reduction purposes, and
- Section 30 of the Greater London Authority Act 1999 (as amended) that provides the Mayor with a general power to act on behalf of the GLA to do anything which he considers will further the promotion of social development in Greater London and to promote improvements in the health of persons in Greater London.

For SafeStats, the Article 6 legal basis (under GDPR) for processing identifiable personal data falls under article 6(1)(e)-

> *processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*

Section 8(e) of the Data Protection Act 2018 prescribes that the reference Article 6(1)(e) of the GDPR to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority includes processing of personal data that is necessary for the exercise of a function conferred on a person by an enactment or rule of law.

Similarly, where the processing of any identifiable personal data concerning the health of an individual constitutes 'special category' personal data, such processing meets the condition in paragraph 6, Part 2 of Schedule 1 of the 2018 Act (and hence the requirement in Article 9(2)(g) of the GDPR):

> *processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest.*

Both section 8(e) and paragraph 6, Part 2 of Schedule 1 of the 2018 Act have been considered to apply by virtue of the legislation already detailed above, namely;

- Section 115 of the Crime and Disorder Act 1998,
- Section 17 of the Crime and Disorder Act 1998, and
- Section 30 of the Greater London Authority Act 1999 (as amended)

The second data protection principle under article 5(1) of GDPR states that personal data shall be:

> b) *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;*

It is felt that this shows that SafeStats has a clear and defined purpose for processing personal data, which is aligned to an appropriate legal basis for that processing.

Article 5(1)(b) goes on to state that;

> *'..further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes'*;

This is understood that if the personal data was originally processed for a relevant task or function, a separate lawful basis for any further processing for scientific research purposes or statistical purposes is not required.

Article 89 of GDPR sets out the appropriate safeguards and derogations relating to processing for such purposes:

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.
2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

Section 19 of the 2018 Act also provides:

1) This section makes provision about—
    a) processing of personal data that is necessary for archiving purposes in the public interest,
    b) processing of personal data that is necessary for scientific or historical research purposes,
    c) processing of personal data that is necessary for statistical purposes.
2) Such processing does not satisfy the requirement in Article 89(1) of the GDPR for the processing to be subject to appropriate safeguards for the rights and freedoms of the data subject if it is likely to cause substantial damage or substantial distress to a data subject.

SafeStats interpretation of the legislation is as the data providers who collect the data collect it in line with their own established public function, the processing of that data for SafeStats – which either constitutes as scientific research or statistical purposes – would not be incompatible with that original purpose, providing we adhere to Article 89 of GDPR and section 19 of the 2018 Act.

Without providing otherwise-unavailable data in a single location, fully cleansed and comparable, the aim of ensuring that users can conduct efficient analysis would not be met. The time and resources that users would have to spend a) sourcing the data from individual provider organisations possibly multiple times for each user organisation (and the relevant governance that they would require), and then b) cleaning, reformatting the data to suit their analysis would be hugely prohibitive in their influencing of crime reduction activity.

These benefits have been assessed against the wider potential risks to data subjects outlined elsewhere in the DPIA, and it is felt that these benefits outweigh the risks. As previously noted, the risks to individuals are limited due to the minimum pseudonymised data requested from providers, the comparison with publicly-available data, the access breadth of SafeStats' staff access and the limited circumstances under which an individual can be identified.

Any adjustment to the processing to make the method less invasive would rely on the removal of relevant data completely or the further suppression of pseudonymised information. This would disproportionally impact on the key benefits and uses of the data.

5. Identification of Risk

Describe the source of risk and nature of potential impact on individuals.	**Likelihood of harm (1-5)**	**Severity of harm (1-5)**	**Overall risk (1-25)**
A data breach **into** GLA systems from an external party at point of data transfer enabling access to the collated data and therefore the potential identification of an individual. Possible methods:			
1) Data transfer via email	3	4	12
2) Data transfer via secure webmail	1	4	4
3) Data transfer via cloud bucket	2	4	8
Out of scope or identifiable data is provided in the data supply, which could include unrequested personal data and is not picked up by automated QA process	2	5	10
The transfer of data post-receipt to processing pick-up locations requires human involvement and risks errors in onward processing and therefore data analysis	1	2	2
Processing errors during the automated extract-transform-load process and the impact on data accuracy and therefore data analysis	2	3	6
A data breach **within** GLA systems from an internal party, enabling access to the collated data in storage locations and therefore the potential identification of an individual.	1	5	5
Matching of provided datasets within SafeStats (potentially in conjunction with open source sources) by SafeStats staff with access to the source database enabling the identification of an individual.	1	5	5
A data breach **into** GLA systems from an external party through public-facing web application enabling access to the collated data and therefore the potential identification of an individual.	2	5	10
Incorrect onward use of data by user organisations outside the remit of the conditions of use of the data/website enabling the identification of an individual.	3	5	15
Downtime of the system affecting the availability of data and follow-on impact on analysis, or ability to process a rights request	2	1	2
Due to the limited data held by SafeStats for the data subjects featured within the hosted data, it is generally accepted that the SafeStats team has an inability to facilitate the rights of unidentified data subjects.	1	1	1
Inappropriately managed data storage and data retained for longer than is necessary increases the likelihood of inaccurate and outdated data being used as well as creates a greater security risk.	2	4	8

6. Risk reduction measures

Risk	**Measures to reduce or eliminate risk**	**Result: is the risk eliminated, reduced or accepted?**	**Measure approved?**
A data breach **into** GLA systems via:			
• Data transfer via email	• Continually encourage data providers to use one of the alternative more secure methods • Offer guidance/training on these other methods • Ensure supplied data is password protected • Continually make relevant program managers/SRO aware of insecure transfer method.	Accepted	Yes
• Data transfer via secure webmail	• Ensure webmail account (and its access details) are only accessible only by the minimum required persons • Ensure supplied data is password protected • Ensure webmail account details are stored securely.	Reduced	Yes
• Data transfer via cloud bucket	• Ensure cloud bucket account (and its access details) are only accessible only by the minimum required persons • Ensure supplied data is password protected • Ensure cloud bucket account details are stored securely.	Reduced	Yes
Out of scope or identifiable data provided	• First-stage human visual check that data structure and potentially personally identifiable fields are as expected (e.g. freetext location of incident) • Second-stage automated QA covering data shape, size, spread, field names • Final-stage human visual dip check of potentially personally identifiable fields • Data provider will be immediately notified, and a replacement dataset sought, with the original deleted (taking into consideration the GLA deletion policy).	Reduced	Yes
Human involvement in the transfer of data post-receipt	• Transfer process limited to only a single 'drag and drop' step • Visual check to ensure correct data has been 'dropped' • Only occurs where data is supplied via email, so same measures as for this risk (above) are implemented.	Reduced/Eliminated	Yes
Processing errors during the automated extract-transform-load process	• Processing scripts continually tested over course of 12 months to ensure used functions are stable and outputs are always as expected when data structure is correct • QA script step ensures that that structure is as expected prior to processing • All scripts independently assessed on an ad-hoc basis for potential efficiency savings, bugs and weaknesses.	Reduced	Yes
A data breach **within** GLA systems	• Access to cloud storage and live database within GLA VPN restricted to SafeStats staff and GLA Technology Group only • Access details stored in secure location where only some staff have access.	Reduced/Eliminated	Yes

Matching of provided datasets by SafeStats staff	• Database and superadmin web application access restricted to only SafeStats staff who have a data processing role (2) • Training provided to staff as to appropriate use of data.	Reduced/Accepted	Yes
A data breach **into** web application and component GLA systems	• Full independent penetration and security testing carried out (and passed) on web application • Full independent penetration and security testing carried out (and passed) on GLA server hosting web application • Rigorous adherence to all GLA security policies, including those that dictate the management of operating system updates on both GLA servers and network infrastructure • Regular maintenance sprints run by the GLA-support partner to ensure all modules and security updates are deployed to LGov and microsites • SafeStats and associated data is backed up regularly to protect against the loss of personal data • Minimum password complexity rules for all SafeStats accounts.	Reduced	Yes
Incorrect onward use of data by user organisations	• For access, senior manager in user organisation attests to suitability of user for access (stored by SafeStats) • On each access, user attests to compliance to conditions of use of data (stored by SafeStats) including appropriate onward use of data • Data transparency through thorough metadata for all datasets contained within SafeStats • Only organisations who have a fully signed DSA with SafeStats (Data Controller to Data Controller) are permitted access to SafeStats data • The SafeStats management have formally requested that all organisations who have accessed any personal data under outdated SafeStats data sharing agreements to undertake an audit of their systems and delete any data downloaded and retained while this previous agreement was active • Risk of access removal for user and organisation made clear if breached • SafeStats staff can audit all users' system access, data querying and data downloading activity.	Reduced/Accepted	Yes
System downtime	• For scheduled downtime, out of hours chosen, with consideration of email to users if required. • For unscheduled downtime, Pingdom email alert system set up for key personnel, holding page available, SLA with Developers for investigation and fixes within 48 hours depending on severity of issue, and email to users if required.	Reduced	Yes

Rights Request	- Privacy Policy available on the SafeStats website, which includes the purposes of the processing, and the lawful basis for the processing.	Accepted	Yes
Data storage management and retention issues	- Adherence to the GLA/SafeStats active data retention policy - The SafeStats team periodically review the processing to ensure that the personal data being held is still relevant and adequate for their purposes, and that they delete anything that is no longer need. This due diligence is expected of all SafeStats accessing organisations; with regular reminder communications sent out to the organisational administrators - Strict adherence to the principles of data minimisation.	Reduced/Accepted	Yes

7. Sign-off

Item	Name/date	Notes
Measures approved by:	Vivienne Avery Demography & Policy Analysis Manager GLA (March 2021)	None
DPO advice provided:	Ian Lister Information Governance Manager GLA (March 2021)	None
Summary of DPO advice: None		
DPO advice accepted or overruled by:	Accepted [redacted] GLA	None
Comments: None		
This DPIA will be kept under review by:	[redacted] GLA	None