



Cabinet Office

**GOV.UK Notify**

**Data Processing and  
Financial Agreement**

**Crown Bodies**

**Version 5.3**

# DATA PROCESSING and FINANCIAL Agreement for GOV.UK NOTIFY

**THIS Agreement** is made between:

**THE GOVERNMENT DIGITAL SERVICE**, a division of the Cabinet Office, of White Chapel Building, 10 Whitechapel High Street, London E1 8DX ("**GDS**")

**AND**

The "**Customer**", a public sector organisation (and together with GDS the "**Parties**").

## **BACKGROUND:**

- A. The public sector receives millions of calls every year from people anxious to find out about the progress of their application or whether we received their payment. People have to spend time on hold, which wastes their time and costs the public sector a lot of money in call centre running costs. Likewise, the costs for other correspondence initiated by public sector organisations, can be significant as individually they may not have the volumes to attract the best prices.

GOV.UK Notify makes it easier to keep people updated, by helping service teams across the public sector to send text messages, emails or letters to their Users. GOV.UK Notify provides an improved and more centralised means by which organisations can send messages (text message, email and post) to the citizens that use their services. The notifications typically take the form of status updates, requests for action, acknowledgement of receipt of applications or supporting information, and reminders.

GOV.UK Notify is not a contact database for UK citizens. The Customers will continue to collect, manage and control the contact information and preferences for their Users. GOV.UK Notify simply Processes the messages to Users at the request of the service team.

The Customer will pass Personal Data to Notify in order to complete the Processing. This Data Processing and Financial Agreement covers this transfer.

- B. The Customer will be legally responsible for compliance with the data protection principles under the UK GDPR and the Data Protection Act 2018 in relation to the Notify Data, and GDS as the public sector organisation's Processor will comply with the applicable Data Protection Legislation while Processing the public sector organisation's Notify Data. This Agreement exists to provide a framework for that compliance.

**IT IS NOW AGREED** as follows:

## **1. DEFINITIONS AND INTERPRETATION**

- 1.1 In this Agreement the following words and phrases shall have the following meanings, unless expressly stated to the contrary:

**Agreement:** this Memorandum of Understanding;

**Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Data Protection Officer** take the meaning given in the UK GDPR;

**Clauses** means the main body of this Agreement excluding Annexes;

**Customer** has the meaning given to it in page 2 of this Agreement;.

**Data Loss Event:** any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach;

**Data Protection Impact Assessment (DPIA)** means an assessment by the Controller on the impact of the envisaged Processing on the protection of Personal Data;

**Data Protection Legislation:** means:

- (i) the UK GDPR as amended from time to time;
- (ii) the DPA 2018 to the extent that it relates to the processing of personal data and privacy;
- (iii) (to the extent that it applies) the EU GDPR; and
- (iv) all applicable Law relating to the processing of personal data and privacy;

**Data Subject Request:** a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation;

**DPA 2018:** Data Protection Act 2018;

**Environmental Information Regulations** means the Environmental Information Regulations 2004, as amended, or Environmental Information Regulations (Scotland) 2004 (as appropriate), together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government Department in relation to such regulations;

**EU GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it has effect in EU law;

**FOIA** means the Freedom of Information Act 2000, as amended;

**FOISA** means the Freedom of Information (Scotland) Act 2002;

**Free Text Message Allowance** means the volume of text message which the Customer may send via GOV.UK Notify without charge as set out in the Pricing Information.

**IAO** means Information Asset Owner, namely the individual occupying the position of Information Asset Owner within the Customer organisation, who has asset ownership obligations in relation to the Notify Data;

**Law:** means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, right within the meaning of the European Union (Withdrawal) Act 2018 as amended by European Union (Withdrawal Agreement) Act 2020, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the Customer is bound to comply;

**LED:** Law Enforcement Directive (*Directive (EU) 2016/680*);

**Notify Data** means all Personal Data passed by the Customer to GDS for the purposes of the Customer's use of GOV.UK Notify Project as provided for in this Agreement;

**Notify Project** means the GOV.UK Notify Project summarised in point A of 'Background' above and in Clause 7 of this Agreement;

**Party** means a Party to this Agreement;

**Pricing Information** means the pricing information set out at <https://www.notifications.service.gov.uk/pricing> as updated from time to time

**Processor Personnel:** means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Agreement;

**Protective Measures:** appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Clause 10;

**Request for Information** means a request for information or a request under FOIA or the Environmental Information Regulations;

**Sub-Processor:** any third party appointed to Process Personal Data on behalf of that Processor related to this Agreement;

**Terms of Use** means the [Terms of Use](#) that each digital service managed by the Customer will be required to accept before connecting to the Notify Project;

**User** means the Data Subject receiving emails, text messages, or letters via the Notify Project; and

**UK GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, together with the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019

1.2 In this Agreement:

- (a) the masculine includes the feminine and neuter;
- (b) person means a natural person;
- (c) the singular includes the plural and vice versa;
- (d) a reference to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or instrument or as contained in any subsequent re-enactment.

1.3 Headings are included in this Agreement for ease of reference only and shall not affect the interpretation or construction of this Agreement.

1.4 References in this Agreement to Clauses, Paragraphs and Annexes are, unless otherwise provided, references to the Clauses, Paragraphs and Annexes of this Agreement.

1.5 In the event and to the extent only of any conflict or inconsistency between:

- (a) the provisions of the Clauses and the provisions of the Annexes, the provisions of the Clauses shall prevail; or
- (b) the provisions of this Agreement and the provisions of any document referred to or referenced herein, the provisions of this Agreement shall prevail.

## **Agreement ACCEPTANCE INSTRUCTIONS**

GDS shall publish the latest version of this Agreement pack on the GOV.UK Notify website and this can be viewed at <https://www.notifications.service.gov.uk/Agreement/crown>. Each Customer shall then accept the Agreement when they make a 'request to go live' on the Notify website.

The Agreement covers all digital services within the Customer organisation that will use Notify. As such, only the first of those digital services will be prompted to accept these Agreement.

The Customer will provide the name and contact details of the person accepting the Agreement, along with the version number of the Agreement pack they are accepting. The person accepting the Agreement must be authorised to enter contracts on behalf of the Customer.

GDS shall then record:

1. The name and email address of the person accepting the Agreement pack on behalf of the Customer
2. The version of the Agreement pack being accepted by the Customer
3. The date and time the Agreement pack was accepted

The Agreement becomes effective once it has been accepted by the Customer. GDS will then email the person formally accepting the Agreement to confirm the Agreement is in place.

## **2. PURPOSE**

- 2.1 The main aims of the Notify Project are: to simplify the process by which citizens, businesses, public sector employees, and elected officials are kept informed about applications, transactions or other interactions they have with public sector organisations. This reduces the costs of correspondence issued by public sector organisations. By moving from the current diverse delivery mechanisms owned and operated by individual service teams to a centralised conduit for delivery of messages (GOV.UK Notify), it will be possible to provide citizens with an improved service over a wider range of mediums than previously available.
- 2.2 It is envisaged that this will result in a marked reduction in the volume of phone calls and post that public sector organisations are currently required to answer, in response to citizens seeking updates e.g. 'has my application been received?' or 'what documentation do I need to submit?'. There is a recognised significant financial benefit associated with proactively keeping citizens informed through the use of very low cost communications when compared with the high cost of fielding phone calls and post through the use of contact centres.
- 2.3 There are also significant savings to be made through the economies of scale that a shared platform can achieve. The unit prices for sending email, text messages and letters through Notify will often be significantly lower for service teams than their existing prices.
- 2.4 The public sector organisation needs to share Notify Data with GDS as its Processor for this service to be provided effectively by GDS.

## **3. COMMENCEMENT, TERM AND VARIATION**

- 3.1 This Agreement shall commence upon acceptance by the Customer and shall continue in effect until the Notify Project terminates unless otherwise subject to earlier termination in accordance with Clause 14.
- 3.2 Variations to this Agreement can be made from time to time by GDS. An updated version of the Agreement will be emailed to the Customer 30 days in advance of any variation taking effect, along with a summary of the changes. Subject to Clauses 3.3 and 3.4 the new Agreement will then take effect after these 30 days. No action is required by the Customer if they accept the updated Agreement.
- 3.3 If the Customer wishes to propose further changes to the updated Agreement, they can send these to GDS by email. Any proposed changes will need to be discussed and agreed by both Parties. A further updated Agreement will then be emailed to the Customer for acceptance by the date the original variation would have taken effect.
- 3.4 The Customer must notify GDS by email prior to the variation taking effect in accordance with Clause 3.2 if they do not wish to accept an updated Agreement. Where the Customer has given such notification this Agreement will automatically terminate on the date the original variation would otherwise have taken effect.

#### **4. REPRESENTATIVES**

- 4.1 The Parties will each appoint a representative to be the primary point of contact in all matters relating to this Agreement:

**For GDS:**

Irina Pencheva  
Lead Product Manager  
irina.pencheva@digital.cabinet-office.gov.uk  
0782 355 29 40

**For the Customer:**

The person that accepts this Agreement, using the contact details provided at the time of acceptance.

- 4.2 The group who will be supervising the Processing of the Notify Data is the GOV.UK Notify team within GDS.
- 4.3 The groups who will be Processing the Notify Data are the GOV.UK Notify team within GDS.
- 4.4 The Sub-Processors who will be Processing the Notify Data as at the date of acceptance of this Agreement are attached to this document in Annex A.
- 4.5 GDS will inform the Customer whenever it appoints or removes a Sub-Processor Processing Notify Data by emailing the Customer's appointed representative named in Clause 4.1 above. Changes to Sub-Processors will be handled in accordance with Clauses 10.10 and 10.11.

#### **5. SUPPLIER CHARGES**

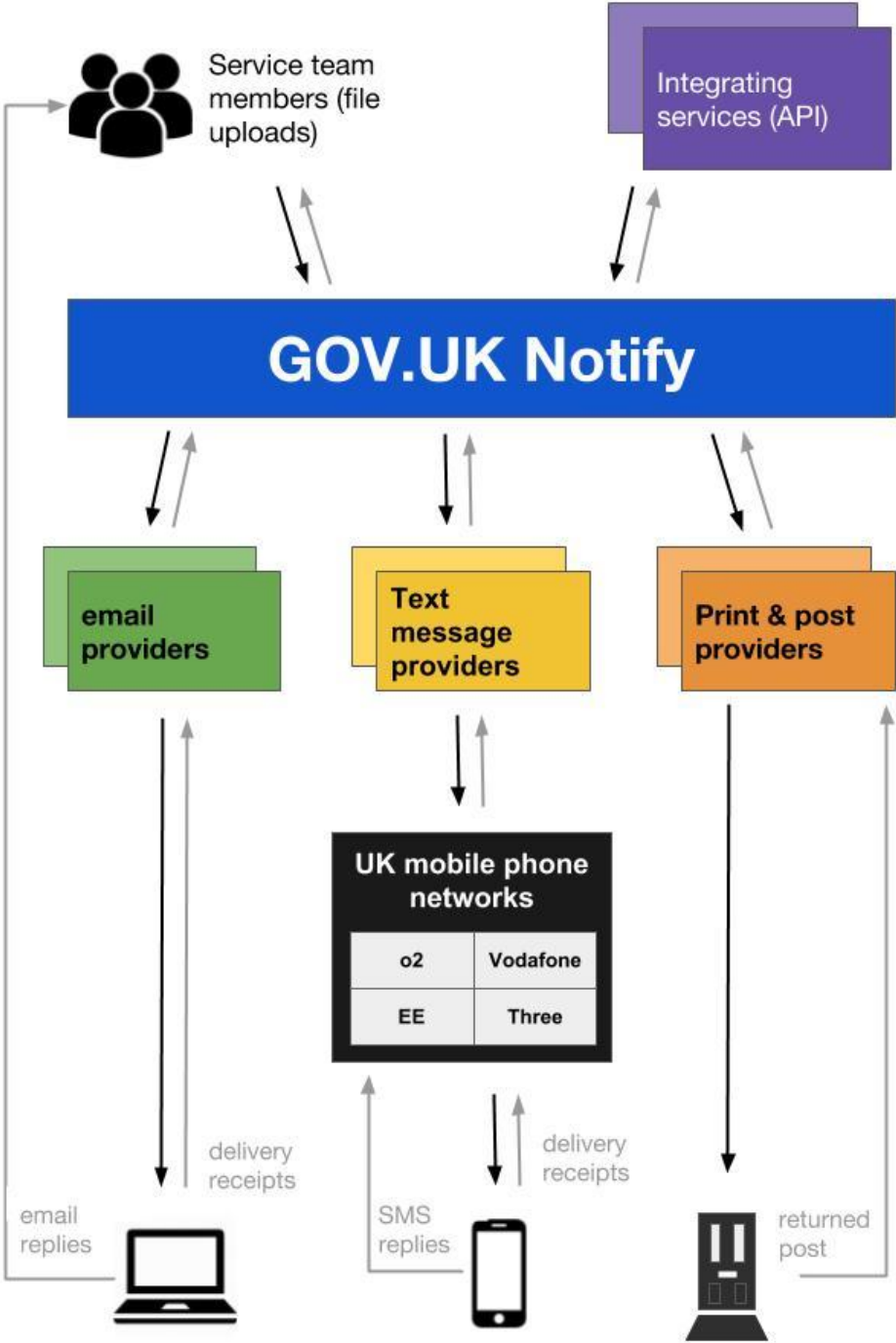
- 5.1 The Customer will pay for all text messages above the Free Text Message Allowance and all letters sent through GOV.UK Notify at the prices as set out in the Pricing Information. The Customer acknowledges that GOV.UK Notify is made available at rates which GDS' suppliers charge which may be subject to change arising from external factors or change of supplier. GDS will endeavour to mitigate any adverse changes but reserves the right to change the pricing and Pricing Information accordingly.
- 5.2 An invoice from GDS and Cabinet Office finance team, showing Notify usage, will be sent to Customers on a quarterly basis. This invoice will provide a breakdown by each of the digital services within the Customer organisation that has incurred a cost.
- 5.3 Payments should be made promptly within 30 calendar days of receipt of invoice.

- 5.4 Details on how to pay are provided on the Notify website and can be viewed at <https://www.notifications.service.gov.uk/pricing/how-to-pay>
- 5.5 A purchase order for the financial year, or confirmation invoices can be received without a purchase order reference, should be shared with the Cabinet Office within the first month of usage.
- 5.6 Failure to provide a purchase order, or to pay an invoice, may result in suspension of access to Notify for the Customer organisation, or specific services within the Customer organisation.

## **6. NOTIFY DATA**

- 6.1 Figure 1 below outlines the Notify Data flows and transfer method to be used for the Notify Project:

*Figure 1: Notify Data flows and data transfer method:*



## **7. THE NOTIFY PROJECT**

7.1 Service teams within public sector organisations will identify opportunities within their service to send emails, text messages or letters to recipients, proactively updating them on progress.

7.2 There are 3 ways for the Customer's service teams to send messages through Notify.

- 1) By integrating their systems with Notify and automatically sending the messages;
- 2) Members of the service team will log in the Notify administration system and upload batches of data collected lawfully or extracted from their back office systems;
- 3) Members of the service team will log in the Notify administration system and type in the details to send one-off messages.

7.3 For email and text messages – the Customer's service team members need to set up templates in the Notify admin application. These templates are checked at the Notify team's discretion before a service can send their first messages, to ensure they won't be used to send unsolicited messages. When they then trigger messages to be sent, either through the integration, or by uploading data, they provide the Personal Data required to construct the message, and nominate the template to insert that data into for sending.

Notify then assembles the email or text messages, by combining the template with the Personal Data (this will include a mobile telephone number and/or email address and other information for each recipient).

7.4 For letters – the Customer's service team members choose to either set up templates in the Notify admin application or pass fully assembled letter content to Notify directly. In either case, the content will be checked for quality at the Notify team's discretion.

Where letter templates are used, Notify then assembles the letter, by combining the template with the Personal Data (this will include name, postal address and other information for each recipient).

7.5 The assembled messages (whether they be email or text messages or letters) are then passed by Notify to the 3rd party suppliers for delivery via email, SMS or post. These suppliers deliver the messages and provide a delivery success update to Notify. Service teams can then query Notify to gain an acknowledgement of delivery (or a failure reason).

7.6 The acknowledgement can be automatically collected by the integrated system, or service team members can see the outcome in the Notify administration application. Once the outcome has been made available to the service, then the limited Personal Data that is held by GDS and the 3rd party providers is deleted in line with their various data retention policies (See Annex B).

7.7 Notify retains data as set out in Annex B. Notify will not analyse Notify Data in any way which would link messages received by a single User, or any subset of Users, from multiple Customers.

- 7.8 GDS commits to work with service teams within devolved administrations, to meet and incorporate their requirements for Welsh Language functionality and support.

## **8. LEGAL BASIS**

- 8.1 The Customer as Controller is responsible for ensuring that:

- a. it is permitted by Law to transfer the Notify Data to GDS as its Processor;
- b. it has the User's consent, where necessary, to transfer the Notify Data to GDS and for GDS and its Sub-Processors to transmit a message by email, SMS or post to the User; and
- c. it complies with the Data Protection Legislation and other applicable data protection Law for each of the Data Subjects. This will include ensuring the Personal Data is kept up to date, and only retained for as long as required.

- 8.2. This Agreement is a Memorandum of Understanding which sets out a formal Agreement between Crown bodies. However, it is not a contract and may not be enforced in the courts. Any dispute will be escalated to appropriately senior officers of GDS and the Customer for resolution.

- 8.3 This Memorandum of Understanding is intended to comply with UK GDPR Article 28 and/or DPA 2018 section 59, pursuant to section 209(3) of the DPA 2018.

## **9. FURTHER USE OF NOTIFY DATA**

- 9.1 GDS agrees not to undertake Processing of Notify Data, except as necessary for the performance of the Notify Project as set out in paragraph 7 and to achieve the purposes in paragraph 2 and in accordance with the Customer's requirements set out in the Schedule of Processing, Personal Data and Data Subjects.

## **10. PROTECTION OF PERSONAL DATA**

- 10.1 The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and GDS is the Processor. The only Processing that GDS is authorised to do is listed in Schedule 5 by the Customer and may not be determined by GDS.
- 10.2 GDS shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the applicable Data Protection Legislation.
- 10.3 GDS shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Customer, include:
- (a) a systematic description of the envisaged Processing operations and the purpose of the Processing;
  - (b) an assessment of the necessity and proportionality of the Processing operations;
  - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and

- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

10.4 GDS shall, in relation to any Personal Data processed in connection with its obligations under this Agreement;

- (a) process that Personal Data only in accordance with Schedule 5 unless GDS is required to do otherwise by Law. If it is so required GDS shall promptly notify the Customer before Processing the Personal Data unless prohibited by Law;
- (b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:
  - 1) nature of the data to be protected;
  - 2) harm that might result from a Data Loss Event;
  - 3) state of technological development; and
  - 4) cost of implementing any measures;

10.5 GDS shall ensure that:

- (a) GDS Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule 5);
- (b) It takes all reasonable steps to ensure the reliability and integrity of any GDS Personnel who have access to the Personal Data and ensure that they:
  - 1) are aware of comply with the GDS duties under this Clause
  - 2) are subject to appropriate confidentiality undertakings with GDS or any Sub-Processor;
  - 3) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Customer or as otherwise permitted by this Agreement;
  - 4) have undergone adequate training in the use, care, protection and handling of Personal Data;
- (c) Where the Personal Data is subject to the UK GDPR, it will not transfer Personal Data outside of the United Kingdom unless either:
  - 1) the transfer is in accordance with Article 45 of the UK GDPR or section 17A of DPA 2018; or
  - 2) the prior written consent of the Customer has been obtained and the following conditions are fulfilled:
    - GDS or the Customer has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or section 75 of DPA 2018) as determined by the Customer (which could include could include relevant parties entering into the International Data Transfer Agreement or International Data Transfer Agreement Addendum to the European Commission's SCCs as published by the Information Commissioner's Office), as well as any additional measures determined by the Customer;

- the Data Subject has enforceable rights and effective legal remedies;
  - GDS complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
  - GDS complies with any reasonable instructions notified to it in advance by the Customer with respect to the Processing of the Personal Data;
- (d) Where the Personal Data is subject to the EU GDPR, it will not transfer such Personal Data outside of the European Union unless either:
- 1) the transfer is in accordance with Article 45 of the EU GDPR; or
  - 2) the prior written consent of the Customer has been obtained and the following conditions are fulfilled:
    - GDS or the Customer has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the Customer which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU set out in Annex 3 to Schedule 31 (Processing Personal Data) or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures determined by GDS;
    - the Data Subject has enforceable rights and effective legal remedies;
    - GDS complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
    - GDS complies with any reasonable instructions notified to it in advance by the Customer with respect to the Processing of the Personal Data;
- (e) At the written direction of the Customer, delete or return Personal Data (and any copies of it) to the Customer on termination of the Agreement unless GDS is required by Law to retain the Personal Data.

10.6 Subject to Clause [10.6.3] GDS shall notify the Customer immediately if it:

- 1) receives a Data Subject Request (or purported Data Subject Request);
- 2) receives a request to rectify, block or erase any Personal Data;
- 3) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- 4) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
- 5) receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
- 6) becomes aware of a Data Loss Event.

10.6.1 GDS obligation to notify under Clause 10.6 shall include the provision of further information to the Customer in phases, as details become available.

- 10.6.2 Taking into account the nature of the Processing, GDS shall provide the Customer with full assistance in relation to either party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 10.6 (and insofar as possible within the timescales reasonably required by the Customer) including by promptly providing:
- 1) The Customer with full details and copies of the complaint, communication or request;
  - 2) Such assistance as is reasonably requested by the Customer to enable the Customer to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
  - 3) The Customer, at its request, with any Personal Data it holds in relation to a Data Subject;
  - 4) Assistance as requested by the Customer following any Data Loss Event;
  - 5) Assistance as requested by the Customer with respect to any request from the Information Commissioner's Office, or any consultation by the Customer with the Information Commissioner's Office.
- 10.6.3 GDS shall maintain complete and accurate records and information to demonstrate its compliance with this Clause. This requirement does not apply where the Customer employs fewer than 250 staff, unless:
- 1) The Customer determines that the Processing is not occasional;
  - 2) The Customer determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR;
- or
- 3) The Customer determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 10.7 GDS shall allow for audits of its Data Processing activity by the Customer or the Customer's designated auditor.
- 10.8 GDS shall designate a data protection officer as required by the Data Protection Legislation.

The contact is:

Data Protection Officer  
Cabinet Office  
70 Whitehall  
London  
SW1A 2AS

[dpo@cabinetoffice.gov.uk](mailto:dpo@cabinetoffice.gov.uk)

- 10.9 GDS shall remain fully liable for all acts or omissions of any of its Sub-Processors.

10.10 GDS may change its Sub-Processors from time to time. Before allowing a Sub-Processor to process any Personal Data related to this Agreement, GDS must:

- have undertaken an information security assessment of the Sub-Processor to ensure compliance with all aspects of this agreement;
- have a written agreement with the Sub-Processor which commits them to continued compliance with all aspects of this Agreement;
- notify the Customer in writing of the new Sub-Processor and type of Processing they will undertake in accordance with Clause 5.1;
- provide the Customer with such information regarding the Sub-Processor as the Customer may reasonably require.

GDS will not disclose Notify Data to any outside organisation unless permitted by this Agreement or required by law.

10.11 GDS shall email the Customer's appointed representative named in Clause 4.1, of intended changes concerning the addition or replacement of a Sub-Processor, at least 15 calendar days before the change takes effect.

If the Customer wishes to object to the Sub-Processor change, they must raise this by sending an email to GDS. Any proposed concerns need to be discussed and resolved by both Parties within these 15 days. Resolution may include not proceeding with the change to the Sub-Processor.

If the Parties cannot resolve the objections raised by the Customer, then the Customer must commence termination in accordance with Clause 14.

10.12 The Parties agree to take account of any non-mandatory published guidance issued by the Information Commissioner's Office. The Customer may require that this agreement is updated to comply with any guidance issued by the Information Commissioner's Officer within 30 calendar days of request to GDS.

10.13 GDS will retain Notify Data as indicated in Annex B.

10.14 GDS agrees to process the Notify Data in accordance with the requirements of this Agreement, and in particular GDS agrees that it shall:

(a) process the Notify Data only as set out in this Agreement;

(b) process the Notify Data only to the extent, and in such manner, as is necessary for the Notify Project;

(c) comply with obligations of the applicable Data Protection Legislation and in particular implement appropriate technical and organisational measures to protect the Notify Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall ensure a level of security appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Notify Data and having regard to the nature of the Notify Data which is to be protected;

(d) take reasonable steps to ensure the reliability of any Personnel who have access to the Notify Data, including those set out in Clause 11 of this Agreement;

(e) transfer the Notify Data only to those Sub-Processors listed in Annex A or subsequently notified to the Customer;

(f) ensure that all Personnel required to process the Notify Data are informed of GDS's obligations under this Agreement with regard to the security and protection of Notify Data and that those obligations are complied with;

(g) ensure that no Personnel publish, disclose or divulge any of the Notify Data to any third party unless directed in writing to do so by each of the Parties;

(h) notify the Customer within five working days if it receives a complaint or request relating to the Parties' obligations under the applicable Data Protection Legislation in force;

(i) if it receives a subject access request under the applicable Data Protection Legislation, or any complaint in relation to Notify, to inform the complainant or requester that the Customer is the Controller and ask the User to contact the Customer DPO where appropriate.

10.15 GDS shall comply at all times with the applicable Data Protection Legislation in force and shall not perform its obligations under this Agreement in such a way as to cause the Customer to breach any of its applicable obligations under the applicable Data Protection Legislation and any other law which is applicable to public bodies in general, in particular the Human Rights Act 1998 and the common law of confidentiality.

10.16 The Customer shall ensure that privacy notices for any of their services using Notify are accessible to those service's Data Subjects and are kept up-to-date, accurately describing the processing that will take place in relation to Notify Data.

## **11. SECURITY OF NOTIFY DATA**

11.1 In addition to the requirements in Clause 10 in respect of Personal Data GDS agrees to Process all the Notify Data in accordance with the following security requirements:

- (a) access to the Notify Data (including any part of the Notify Data and any copies), will be restricted to service teams that provided the data to Notify; SC cleared operations staff at GDS supporting Notify during business hours; and the 3rd party suppliers listed in Annex A.
- (b) Notify Data will be protected using secure network protocols such as TLS when it is in transit between Customer systems and Notify; and when it is in transit between Notify and its 3rd party suppliers. The use of TLS to protect emails sent by Notify is opportunistic and relies on the receiving mail server supporting the protocol and strong cipher suites. Notify Data will be encrypted when it is temporarily stored in the Notify data store. The number of named individuals that have access to the systems in which the data passes and is stored will be kept to a minimum.

## **12. FREEDOM OF INFORMATION**

- 12.1 The Parties are all subject to the provisions of FOIA or FOISA (as appropriate) and the Environmental Information Regulations and shall assist and co-operate with each other to enable each other to comply with their respective statutory duties in relation to Requests for Information. In particular, where a Party receives a Request for Information pertaining to the subject matter or operation of this Agreement, it shall as soon as practicable notify the other Party's nominated representative, in writing, of the details of the information requested, the date such Request was made and, if permitted by Law, the name of the person making the Request. The Party which has received the Request shall, prior to responding to the applicant, consult with the other Party and to facilitate such consultation shall provide it with a copy of all information which it proposes to disclose not less than 5 working days before disclosure.

## **13. LOSS AND UNAUTHORISED RELEASE**

- 13.1 GDS will report any Data Loss Event to the Customer, without undue delay, and where possible no later than 24 hours after the loss or unauthorised release is discovered, and within the statutory time limit of 72 hours to allow the parties to meet their obligations.
- 13.2 GDS acknowledges that any loss or unauthorised release of the Notify Data will be valid grounds for the Customer to terminate this Agreement.
- 13.3 Any loss or unauthorised release of the Notify Data by GDS will need to be investigated jointly by all Parties. Existing Customer data incident processes and reporting will be utilised.

## **14. TERMINATION**

- 14.1 Either Party may, for any reason, terminate this Agreement upon three months' written notice to the other.
- 14.2 The Customer must terminate this Agreement, or cease use of Notify, where there are unresolvable objections to proposed Sub-Processor changes, before the advised Sub-Processor changes take effect.
- 14.3 Either Party may terminate this Agreement with immediate effect in the event of breach of its obligations by the other Party to this Agreement.
- 14.4 The Customer shall pay any undisputed charges due under Clause 5.1 within [30 days] of the date of termination.

## Version History

Version	Date	Description
1.0	25 April 2016	Document status elevation after GLD review.
2.0	04 Nov 2016	Updated with information about Notify generating letters.
3.0	26 April 2018	Updated for UK GDPR compliance
4.0	25 June 2019	Updated to reflect the move to online acceptance of the Agreement.
5.0	26 August 2020	Aligned the Defined Terms with Procurement Policy Note (PPN)02/18 Added Sinch UK as an SMS Sub-Processor. Updated process for changing Sub-Processors.
5.1	8 October 2020	Alignment of defined terms throughout Agreement, and clarification of working versus calendar days.
5.2	10 December 2020	Correction of item numbering in the defined term 'Data Protection Legislation'. Clarification that Annex A lists Sub-Processors explicitly, rather than suppliers.
5.3	16 March 2023	Replaced 'GDPR' with 'UK GDPR' and 'EU GDPR' references as required Clarification of Variation process Clarification of data retention of some Sub-Processors

## **ANNEX A - Sub-Processors Processing Notify Data on behalf of Notify**

### **SMS Sub-Processors:**

- MMGRP Ltd (Company number: 7527443): 20-22 Wenlock Road, London N1 7GU, UK - use a Private Cloud provided by Rackspace from data centres located in Crawley and Slough.
- MMGRP Ltd Sub-Processor - Infobip Ltd (Company number: 07085757): Fifth Floor, 35 - 38 New Bridge Street, London EC4V 6BW, UK - includes a custom SMPP engine hosted alongside MMGRP's systems in the UK and an Infobip platform hosted in an Equinix data centre in Frankfurt, Germany.
- FireText (Company number 06280579): Tremough Innovation Centre, Penryn TR10 9TA, UK - use third party data centre facilities in Reading and Manchester which are provided as a Private Cloud by Pulsant Limited
- FireText Sub-Processor - Sinch UK Ltd (Company number: 03049312): Sinch offices in UK: Viking House John Roberts Business Park, Pean Hill Blean Kent CT5 3BJ, UK. Sinch Support offices, Slöjdaregatan 1, 393 53 Kalmar, Sweden. Data centres: EU3C, co-location data centre in Hammerby, Sweden and EU1C, Amazon AWS Europe Data Centre in Dublin, Ireland.

### **Email and Hosting Sub-Processor:**

- Amazon Web Services (Company Number: 08650665): 60 Holborn Viaduct, London EC1A 2FD, UK - Amazon AWS Europe Data Centre in Dublin, Ireland.

### **Letter Sub-Processor:**

- DVLA: Ty Felin, Swansea, SA5 4HH, Wales

### **Out of hours support:**

- UK-based independent SC cleared contractors engaged by GDS via the CCS RM6160 framework

## Annex B – Data retention times

Data retention times for GOV.UK Notify and suppliers.

**Personal Data** includes the mobile number, email address or postal address and the message body. **Non-Personal Data** includes a generated message ID, timestamps and delivery status stored mainly for billing purposes

Organisation	Personal Data retention time	Non-Personal Data retention time
GOV.UK Notify	<b>7 days by default Up to 90 days by request</b>	Indefinite
MMGRP Ltd Text message supplier to Notify	<b>30 days</b>	Indefinite
Infobip Processor to MMGRP Ltd	<b>90 days</b>	Indefinite
FireText Text message supplier to Notify	<b>30 days</b>	Indefinite
Sinch UK Ltd Processor to FireText	<b>12 months</b>	12 months
Vodafone Mobile network operator	<b>30 days</b>	3 years
EE Mobile network operator	<b>7 days</b>	1 year
Three Mobile network operator	<b>90 days</b>	Indefinite
O2 Mobile network operator	<b>90 days</b>	Indefinite
Amazon Web Services Email and hosting supplier to Notify	<b>30 days</b>	Indefinite
DVLA Letter supplier to Notify	<b>60 days</b>	Indefinite

## Schedule of Processing, Personal Data and Data Subjects

Description	Details
Subject matter of the Processing	Notify sends transactional updates and subscription based notifications to the Users of public sector services via email, text message and letter.
Duration of the Processing	<p>Processing is typically complete within 7 days, however there is a potential for service teams to request Notify to retain their notification data for up to 90 days so they can subsequently respond to their Users queries about messages they were sent in the past.</p> <p>Third party suppliers to Notify, that distribute the notifications will retain the data for up to 12 months for audit and billing purposes.</p>
Nature and purposes of the Processing	<p>Notify collects Personal Data only for the purposes of Processing notifications and reporting on the success or failure of delivery.</p> <p>Notify uses a number of third party suppliers to distribute the notifications to recipients.</p> <p>Once the relevant retention period has been reached, Notify data is deleted from Notify and from the third party suppliers.</p> <p>While Notify holds data, service teams that have provided the data in their role of Controller, can see the data within Notify and access the delivery outcomes.</p> <p>The purposes for sending notifications to public sector service Users are many and varied, but generally fall into the categories of progress updates about transactions, reminders of appointments or renewals, alerts about guidance changes or events.</p>
Type of Personal Data	<p>All notifications will contain either an email address, a mobile phone number, or a physical address.</p> <p>Additionally there can be personalisation in the notifications, which can include people's names, reference numbers, dates of events / appointments etc.</p>
Categories of Data Subject	Staff (including volunteers, agents, and temporary workers), elected officials, customers/clients, suppliers, patients, students/pupils, members of the public, users of public sector organisations websites.
Plan for return or destruction of the data once the Processing is complete UNLESS requirement under union or member state Law to preserve that type of data	Personal Data is automatically deleted at the end of the data retention period, which for Notify and its third party providers ranges between 3 days and 12 months. This is the case as part of routine Processing, and at termination of this Agreement.