RE: INDEPENDENT INVESTIGATION INTO INVOLVEMENT BY UNION OFFICERS OR OFFICIALS IN THE OPERATION OF BLACKLISTS IN THE CONSTRUCTION INDUSTRY

DATA SHARING AGREEMENT AND PRIVACY NOTICE

---

1. The parties to this agreement are Unite the Union ("Unite"), Sector Forensics ("SF"), Public Interest Law Centre ("PILC"), and Nick Randall KC of Matrix Chambers and John Carl Townsend of 33 Chancery Lane ("the Investigators").

2. By this agreement Unite agrees to allow:

    a. SF to access and acquire its electronically stored information (ESI) in accordance with Appendix 1, and to provide ESI to PILC in accordance with paragraph 15 of Appendix 1.

    b. PILC to review the ESI so provided to it by SF for the purposes of identifying evidence which may potentially be relevant to the Independent Investigation into Involvement by Union Officers or Officials in the Operation of Blacklists in the Construction Industry ("the Investigation"), the Terms of Reference for which may be found here.

    c. Potentially relevant evidence identified by PILC in accordance with 2.(b) above to be provided by PILC to the Investigators to be processed by them for the purposes of the Investigation.

    d. The Investigators to make such reference to and/or include such evidence as is necessary for the purposes of the Investigation in the report to be produced by the Investigators at the conclusion of the Investigation and to be sent to the General Secretary of Unite the Union (the "**Investigation Report**", as to which see further clause 8.c below). Unless it is necessary to do otherwise, any

personal data derived from evidence obtained pursuant to this Agreement shall be included in the Investigation Report in anonymised form, with use of ciphers where appropriate to differentiate between individuals.

e. A copy of each document cited in the Appendix or Appendices to the Investigation Report shall be provided to the Data Protection Officer of Unite the Union at the time that the Investigation Report is provided to the General Secretary, to be retained by Unite until 31 December 2031.

3. In conducting the processes set out at Appendix 1 SF will be acting in the capacity of a processor under the control of PILC in its capacity as solicitors to the Investigation.

4. Each party to this Agreement is a registered Controller under the Data Protection Act 2018. Subject to the express limitation that any and all personal data processed pursuant to this Agreement shall be processed only for the purposes of the Investigation, each party other than SF shall be a Controller of such data as is processed by that Controller pursuant to this Agreement.

5. Contact details for each party's Data Protection Officer or other relevant employee with responsibility for data sharing pursuant to this Agreement are set out at Appendix 2.

6. Each party confirms that it complies with data protection legislation by:

a. having a lawful basis for processing and sharing personal data.

b. having an appropriate policy document in place in respect of the processing of special category data.

c. ensuring data quality.

d. storing and sharing information securely, with access management controls.

e. having policies and procedures for compliance with data protection legislation including for managing data subject rights and complaints, identifying and managing data breaches/incidents and retention and disposal.

f. ensuring that mandatory training is undertaken regularly by their employees to ensure they are clear and up to date on their responsibilities. Every individual must uphold the principles of this agreement and overarching confidentiality, and seek advice from the relevant Data Protection Officer or other relevant employee who has responsibility for data sharing, when necessary.

g. undertaking appropriate data protection due diligence checks with any contractors/data processors they employ, and ensuring that a written agreement is in place with each data processor, and that all data processors will be bound by this agreement.

h. having written processes for the processing of data to ensure employees use and share personal data in line with data protection law, the data protection principles, and this agreement.

7. Further, each party to this Agreement will ensure due regard for confidentiality in the processing of any data for the purposes of the Investigation.

8. The purposes of Unite sharing data with the other parties in accordance with this Agreement for the purposes of the Investigation as set out in the Terms of Reference and are:

a. To consider allegations that their trade union officials colluded with the construction industry to blacklist workers;

b. To consider data from the Unite computer servers, and other relevant sources of data, to establish whether collusion between trade union officials and the construction industry took place; and

c. To produce the Investigation Report. The Investigation Report will provide details as to whether collusion did or did not take place and make recommendations as to how future misconduct may avoided. The production of this report and the analysis of the relevant data is in the interests of individual workers, trade union members and the trade union movement as a whole.

9. The types of data that may be processed for the purposes of the Investigation in accordance with this Agreement are:

a. **Personal Data** - any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

b. **Special Category Data**, namely personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

c. **Criminal Offences Data**, namely data relating to criminal convictions and offences, including personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing.

10. The lawful basis for Unite sharing Personal Data with the other parties pursuant to this Agreement and for the other parties thereafter to process the Personal Data in accordance with this Agreement are:

    a. Article 6(1)(e) of the UK General Data Protection Regulation ("the **UK GDPR**"), namely processing is necessary for the performance of a task carried out in the public interest; and/or

    b. Article 6(1)(f) of the UK GDPR, namely processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

11. In respect of the processing of Special Category Data and Criminal Offences Data the requisite additional lawful basis for Unite sharing such data with the other parties pursuant to this Agreement and for the other parties thereafter to process such data in accordance with this Agreement are:

    a. In relation to Special Category Data:

        i. Article 9(2)(f) of the UK GDPR, namely that processing is necessary for the establishment, exercise or defence of legal claims; and/or

        ii. Article 9(2)(g) of the UK GDPR, namely that processing is necessary for reasons of substantial public interest. The processing meets the condition set out at paragraphs 10(2)and/or 11(1) and or 11(2) of Part 2 of Schedule 1 to the DPA.

    b. In relation to Criminal Offences Data, Article 10 of the UK GDPR on the basis that the processing is authorised by domestic law because, pursuant to paragraph 33(c) of Schedule 1 to the DPA, it is necessary for the purpose of establishing, exercising or defending legal rights.

12. The processing of Special Category Data pursuant to this Agreement referred to at clause 11(a)(ii) above requires an Appropriate Policy Document ("**APD**") to be in place. The APD is at Appendix 3.

YOUR INFORMATION RIGHTS

13. You have the following rights under data protection law:

    a. The right to be informed about the collection and use of your personal data.
    b. A right of access to your personal data, and the right to request a copy of the information that is held about you and supplementary details about that information – you will be asked to provide proof of your identify and residential address, and you may be asked to provide further details to assist in the provision of such information.
    c. The right to have inaccurate personal data that is processed about you rectified.
    d. The right of erasure – in certain circumstances you have the right to have personal data that is processed about you blocked, erased or destroyed.
    e. the right to object to, or restrict:
        - processing of personal data concerning you for direct marketing
        - continued processing of your personal data
    f. the right of portability of your data in certain circumstances.

    You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, a reasonable fee may be charged if your request is clearly unfounded, repetitive or excessive. Alternatively, in these circumstances, your request may be refused.

    Please note that these rights are subject to certain limitations that exist in law.

14. Please contact the Investigation using the details in Appendix 2 paragraph 1 if you would like to exercise any of these rights or know more about them in so far as they relate to personal data controlled by the Investigation.

15. Please contact Unite using the details in Appendix 2 paragraph 2 if you would like to exercise any of these rights or know more about them in so far as they relate to personal data provided to the Investigation by Unite pursuant to this Agreement.

16. In the event that any party to this Agreement is contacted by any individual in respect of personal data provided to that party and originating from Unite pursuant to this Agreement, the information about that contact will be provided to Unite using the details in Appendix 2 paragraph 2, and Unite will assume responsibility for responding to that individual in respect of that data. Each party agrees to provide Unite with such assistance and information as it requires for these purposes.

17. Any data shared by Unite pursuant to this Agreement shall be retained by the parties for no longer than 31 December 2025 and shall be permanently deleted from all systems operated by the parties (other than Unite) by no later than 31 March 2026.

18. Further information about your information rights is available on the Information Commissioner's Office website: https://ico.org.uk/

WHAT SHOULD YOU DO IF YOU HAVE A COMPLAINT?

19. We hope that you will be satisfied with the way in which we will approach and use your personal data for the purposes of the Investigation. Should you find it necessary, you have a right to raise a concern with or make a complaint to the information regulator, the Information Commissioner's Office: https://ico.org.uk/

20. However, we hope that if you have a complaint about the way:

    a. in which the Investigation handles your personal data, you will in the first instance contact the Investigation using the contact details provided in Appendix 2 paragraph 1.

    b. in which Unite handles your personal data, you will in the first instance contact Unite using the contact details provided in Appendix 2 paragraph 2.

RE: INDEPENDENT INVESTIGATION INTO INVOLVEMENT BY UNION OFFICERS OR OFFICIALS IN THE OPERATION OF BLACKLISTS IN THE CONSTRUCTION INDUSTRY

APPENDIX 1 TO DATA SHARING AGREEMENT

ACQUISITION AND PREPARATION OF DATA

PROVISION OF DATA AND SECURE ACCESS

1. Unite shall provide SF and PILC secure administrative access to the specific servers that host the Email System and the Membership Database as provided at paragraphs 8 and 10 below.

2. Unite shall provide SF an encrypted virtual machine copy of certain servers listed in Table 1 which, for the avoidance of doubt, is confidential and does not form part of this Appendix.

FORENSIC ACQUISITION

3. A forensic acquisition of the electronically stored information (ESI) contained upon the Unite encrypted virtual machines detailed in Table 1 will be made by SF.

4. A forensic acquisition of the ESI contained upon the machines detailed in Table 2 will be made by SF. For the avoidance of doubt, Table 2 is confidential and does not form part of this Appendix. The forensic acquisition is a way of preserving this information in a format suitable to be used in any judicial process.

5. A single copy of each forensic acquisition will be signed and sealed in an exhibits bag, along with the virtual machines supplied by Unite. A SHA1 hash value will be noted for

each forensic acquisition (digital equivalent of a DNA match). Once this process has been completed:

5.1. No further work will be conducted on the sealed items, which will be placed in Secure Storage at SF until not later than 31 March 2026 by which point they must be returned to Unite.

5.2. The original of any virtual machine or machine shall be returned to Unite as soon as practicable thereafter or as otherwise agreed with Unite.

6. Should there be a need to go back to the original source (the snap shot of the Unite servers at the time the copy was made), then this will be possible by using these sealed forensic copies that will provide full continuity should the need arise.

FORENSIC EDISCOVERY PROCESS

STEP 1: Live Trial Search (feasibility study)

STEP 2: Live eDiscovery Search (Emails and Membership Database)

STEP 3: Processing and Non-Live Search of VM File Servers

STEP 4: Provision by SF of results of searches made using keyword search terms provided to it by PILC, being search terms intended to capture information relevant to the Investigation ("the **Key Word Search Terms**") to PILC. For the avoidance of doubt, the Key Word Search Terms do not form part of this Appendix and are confidential.

STEP 1: Live Trial Search

A. Live trial search of the Email System
B. Live trial search of the Membership Database

7. A feasibility study needs to be conducted prior to the live search of the Email System and the Membership Database which will occur at STEP 2, to determine if a live search using Unites servers will return accurate data.

8. A trial search will be conducted by SF using 'test keywords', looking for known data contained upon the systems, to ascertain the accuracy of the data returned when keyword searches are utilised; any anomalies will be noted, and the process used in STEP 2 shall be adapted accordingly.

9. The 'test keywords' used by SF will be taken from previous email communications between SF and Unite in respect of the Investigation.

STEP 2: Live eDiscovery Search (Emails and Database)

A. Live eDiscovery search of the Email System

B. Live eDiscovery search of the Membership Database

10. Searches shall be performed by SF across Unite's live Email System and Membership Database using the Key Word Search Terms.

STEP 3: Processing and Non-Live Search of VM File Servers

11. Using a copy of the forensic acquisition of all items listed in Table 1 apart from items 3, 4, 14, 15 and 16 SF will process all of the data for the purpose of putting it into a form in which searches using the Key Word Search Terms can be conducted on it.

12. Further items shall be forensically acquired and secured by SF for the purposes of the Investigation, and shall also be processed for the purpose of putting the data held on them into a form in which searches using the Key Word Search Terms can be conducted on it. Such items include, old hard disks, DLT Tapes and physical documents as set out in Table 2.

13. The processing stage consists of analysing every file and breaking it down into its constituent parts, carrying out character recognition, expanding compressed files, interpreting file structures (e.g. sharepoint), social media, Interpretation and processing of Internet activity etc.

14. Searches shall be performed by SF across all data acquired pursuant to paragraphs 11 to 13 above using the Key Word Search Terms.

STEP 4: Provision of results of searches to PILC

15. Thereafter, SF shall provide the results of the searches using the Key Word Search Terms to PILC in a searchable eDiscovery format.

RE: INDEPENDENT INVESTIGATION INTO INVOLVEMENT BY UNION OFFICERS OR OFFICIALS IN THE OPERATION OF BLACKLISTS IN THE CONSTRUCTION INDUSTRY

APPENDIX 2 TO DATA SHARING AGREEMENT

CONTACT DETAILS FOR DATA PROTECTION OFFICERS

---

1. The Data Protection Officer for the Investigation contactable on the details below:

   office@pilc.org.uk

   Data Protection Officer

   Public Interest Law Centre

   17 Old Ford Road

   London E2 9PJ

2. The Data Protection Officer for Unite is contactable on the details below:

   dataprotection@unitetheunion.org

   Data Protection Officer

   Legal Department

   Unite the Union

   128 Theobalds Road

   London WC1X 8TN

3. Links to the Privacy Notices for each of the parties to the Data Sharing Agreement are set out below.

   Unite

   Sector Forensics

   Public Interest Law Centre

   Nick Randall KC

   John Carl Townsend

RE: INDEPENDENT INVESTIGATION INTO INVOLVEMENT BY UNION OFFICERS OR OFFICIALS IN THE OPERATION OF BLACKLISTS IN THE CONSTRUCTION INDUSTRY

APPENDIX 3 TO DATA SHARING AGREEMENT

POLICY DOCUMENT – SPECIAL CATEGORY DATA

---

1. Special Category Data processed for the purposes of the Investigation for reasons of substantial public interest requires an APD setting out and explaining procedures for securing compliance with the principles in Article 5 of the UK GDPR and policies regarding the retention and erasure of such personal data.

2. This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018. This is the APD for processing pursuant to clause 11(a)(ii) of the Data Sharing Agreement. It demonstrates that the processing of Special Category Data pursuant to that clause is compliant with the requirements of the UK GDPR Article 5 principles. In particular, it outlines retention policies with respect to such data.

3. As noted at clause 11(a)(ii), Special Category Data is processed for the following purposes in Part 2 of Schedule 1:

    - **Paragraph 10(1)** preventing or detecting unlawful acts and/or
    - **Paragraph 11(1) and (2)** protecting the public against dishonesty

4. The procedures of the Investigation for ensuring compliance with the Article 5 principles are as follows:

5. **Accountability principle.** The Investigation has put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

    a. The appointment of a data protection officer for the purposes of the Investigation.

b. Taking a 'data protection by design and default' approach to our activities.
c. Maintaining documentation of our processing activities.
d. Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
e. Implementing appropriate security measures in relation to the personal data we process

6. **Principle (a): lawfulness, fairness and transparency.** Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

7. We have provided clear and transparent information about how and why Unite will provide the Investigation with personal data and about how the Investigation processes personal data including our lawful basis for processing in the Data Sharing Agreement and in this policy document.

8. This processing for purposes of substantial public interest is necessary for the purposes of the Investigation in accordance with the Terms of Reference.

9. **Principle (b): purpose limitation.** Personal data is processed for purposes of substantial public interest as explained above in order to protect the public from dishonesty, and/or prevent or detect unlawful acts, but only for the purposes of the Investigation as defined by the Terms of Reference. We may process personal data collected for any one of these purposes (whether by us or another controller), for any of the other purposes here, providing the processing is necessary and proportionate to that purpose. We will not process personal data for purposes incompatible with the original purpose it was collected for.

10. **Principle (c): data minimisation.** As provided for in the Data Sharing Agreement, the parties have ensured that such personal data as is to be processed for the purposes of the Investigation is necessary for the relevant purposes and is not excessive. The

information we process is necessary for and proportionate to our purposes. Any personal data provided that is not relevant will be erased in accordance with clause 2(c).

11. **Principle (d): accuracy.** Where any party to the Data Sharing Agreement becomes aware that personal data being processed for the purposes of the Investigation is inaccurate or out of date, having regard to the purpose for which it is being processed, that party will provide notification to PILC of the same as soon as reasonably practicable and PILC we will take every reasonable step to ensure that, to the extent that it is held for the purposes of the Investigation, that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

12. **Principle (e): storage limitation.** All special category data processed for the purpose of substantial public interest is to be retained for the period set out at clause 17 of the Data Sharing Agreement.

13. **Principle (f): integrity and confidentiality (security).** Electronic information is processed within secure networks. Hard copy information is processed in line with security procedures. All electronic systems and physical storage systems utilised for the purposes of the Investigation have appropriate access controls applied.

14. The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

15. **Retention and erasure practices.** The applicable retention and erasure practices are set out at clause 17 of the Data Sharing Agreement and paragraphs 10 and 12 above.

16. **Duration of policy**. This policy will be retained for the duration of our processing and for 6 months after processing ceases.