Expol

RISK MITIGATION & FORENSIC INVESTIGATIONS

Data Protection and Privacy Policy for Expol Ltd and ExpolCheck Ltd

("Expol")

Reviewed: November 2023

[For international investigative services, General Data Protection Regulation compliant]

Expol Limited and ExpolCheck Limited https://www.expol.co.uk

Expol

RISK MITIGATION & FORENSIC INVESTIGATIONS

1. The purpose of this Policy is to protect the rights and privacy of living individuals and to ensure that personal data is not processed by *Expol Ltd and ExpolCheck Ltd ("Expol")* without the person's knowledge or consent, unless otherwise exempt.

2. This document sets out the Data Protection Policy for *Expol.*

3. *Expol* complies with the requirements of the prevailing data protection legislation with regard to the collection, storage, processing and disclosure of personal information and is committed to upholding the core data protection principles.

4. *Expol* is committed to a policy of protecting the rights and privacy of individuals (includes staff, course delegates, clients, subjects of investigations, subjects of employment screening services and others) in accordance with the data protection legislation.

5. *Expol* needs to process certain information about its staff, trainees, sub-contractors and other individuals it has dealings with such as clients, for administrative purposes (e.g. to recruit and pay staff) and subjects of investigations and employment screening services and to comply with legal obligations and government requirements.

6. During the course of its core business activities *Expol* will be instructed to process the personal data of individuals who are identified in clients' instructions or during the course of the investigation undertaken pursuant to such instructions. *Expol* **will not process any personal data**
   (a) without first having undertaken a Data Privacy Impact Assessment, and
   (b) without the explicit CONSENT of the data subject, or
   (c) unless there is a specific legitimate interest except where such interests are overridden by the interests or fundamental rights of the data subject, or
   (d) the circumstances are exempt, or
   (e) *Expol* has exemption.

   Furthermore, to comply with the law, information processed about individuals must be kept to the minimum, collected and used fairly, be accurate, used solely for the purpose intended, stored safely, securely including protection against unauthorised or unlawful processing, loss, destruction or damage, using appropriate technical measures such as encryption or in password protected devices, retained for no longer than necessary and not disclosed to a third party unlawfully.

7. As a matter of good practice, other agencies and individuals working with and thus affiliated to *Expol* and who have access to personal information, will be expected to have read and comply with this policy, the terms of which form part of the consultancy/agency agreement between *Expol* and that affiliate. Where data is to be transferred to other jurisdictions it can only occur if that other jurisdiction has laws in place compliant or compatible with the EU General Data Protection Regulation. We use a third party provider to carry out Criminal Checks, based in the United Kingdom. We may change this provider at any time. In the interests of transparency, the details of the current provider may be supplied to our clients and potential clients by contacting us directly.

8. *Expol* is the Data Processor under the data protection legislation, when dealing with its core business as an Investigation Agency, Employment Screening Service, Trainer and/or Security Consultant and the client is the Data Controller.

9. *Expol* is the Data Controller under the data protection legislation, when dealing with data of staff, clients, contractors, trainees and any other member or affiliate of *Expol.* For this purpose, *Expol* has duly Notified the Isle of Man Information Commissioner under registration number **R000721.**

10. The Directors and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within *Expol.*

11. Compliance with data protection legislation is the responsibility of all members and affiliates of *Expol* who process personal information.

12. Each member of staff, clients, contractors, trainees and any other member or affiliate of *Expol* is responsible for ensuring that any personal data supplied to or handled by *Expol* is accurate and up to date.

13. Wherever possible or unless exempt, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent.

14. *Expol* understands “consent” to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

15.

16. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from no response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

17. In most instances consent to process personal and sensitive data is obtained routinely by *Expol* (e.g., when a member of staff or consultant signs a Service or Consultancy Agreement).

18. Any *Expol* forms (whether paper-based or electronic-based), that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data is to be published on the Internet as such data can be accessed from all over the globe.

19. If an individual does not consent to certain types of processing, appropriate action must be taken to ensure that the processing does not take place, unless an exemption applies. **CONSENT GIVEN CAN BE WITHDRAWN AT ANY TIME BY GIVING EXPOL WRITTEN NOTICE.**

20. If any member of affiliate of *Expol* is in any doubt about these matters, they should consult the Directors.

21. All staff and affiliates of *Expol* are responsible for ensuring that any personal data (on others), which they hold are kept securely and that they are not disclosed to any unauthorised third party.

22. All personal data should be accessible only to those who need to use it. Those concerned should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:
    - ➢ In a lockable room with controlled access, or
    - ➢ In a locked drawer or filing cabinet, or
    - ➢ If electronic, cloud based, password protected or,
    - ➢ Kept on disks or other devices which are themselves kept securely.

23. Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screensavers and manual records should not be left where they can be accessed by unauthorised persons.

24. Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

25. This policy also applies to staff and affiliates of *Expol* who process personal data "off- site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and affiliates of *Expol* should take particular care when processing data at home or in other locations outside the offices of *Expol* or its affiliated locations.

    Members of *Expol* and/or other data subjects have the right to access any personal data which are held by *Expol* in electronic format and manual records which form part of relevant filing system held by *Expol* about that person.

26. Any individual who wishes to exercise this right may either request this verbally or in writing including electronic means to the Directors. Expol will make no charge for data subject access requests. Any such request will normally be complied within one month from the next day following the receipt of the request, or one month from the next day following receipt of satisfactory proof of identity if requested.

27. *Expol* must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police, unless authorised under the terms of the prevailing data protection legislation or other statute or Court Order or where disclosure of data is required for the performance of *Expol* contractual duty or otherwise exempt. All staff and affiliates should exercise caution when asked to disclose personal data held on another individual to a third party.

28. The prevailing data protection legislation permits certain disclosures without consent to a Competent Authority, such as law enforcement agencies.

29. For reasons of personal security and to protect *Expol* premises and the property of staff, trainees and other visitors, closed circuit television cameras may be in operation in several areas. The presence of these cameras may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:

    - ➢ Any monitoring will be carried out only by a limited number of specified staff;
    - ➢ The recordings will be accessed only by the Directors of Expol;
    - ➢ Personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete;
    - ➢ Staff involved in monitoring will maintain confidentiality in respect of personal data.

Expol

RISK MITIGATION & FORENSIC INVESTIGATIONS

Definitions

Personal Data

Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller, includes name, address, telephone number, identity number and other identifying data such as a person's DNA. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of individual.

Sensitive Data

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data is subject to much stricter conditions of processing.

Data Controller

Any person (or organisation) that makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data is processed and the way in which the personal data is processed.

Data Subject

Any living individual who is the subject of personal data held by an organisation.

Processing

Any operation related to organisation, retrieval, disclosure and deletion of data includes obtaining and recording data, accessing, altering, adding to, merging, deleting data Retrieval, consultation or use of data Disclosure or otherwise making available of data.

Third Party

Any individual/organisation other than the data subject, the data controller (for example clients) or its agents.

Relevant Filing System

Any paper filing system or other manual filing system, which is structured so that information about an individual is readily accessible. **Please note that this is the definition of "Relevant Filing System".**

Personal data as defined as, and covered by the Prevailing data protection legislation can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from the individual's information can be readily extracted.

Expol

RISK MITIGATION & FORENSIC INVESTIGATIONS

Principles

All processing of personal data must be done in accordance with the six data protection principles.

1. **Personal data shall be processed fairly, lawfully and transparently.**
   Data processing will not be lawful unless it satisfies at least one of the following processing conditions:
   - ➢ **Consent –** The data subject has provided valid consent for the processing.
   - ➢ **Contract –** The processing is necessary for the performance of a contract.
   - ➢ **Legal obligation –** The processing is necessary for compliance with a legal obligation to which the controller is subject.
   - ➢ **Legitimate interest –** The processing is necessary for the purposes of the legitimate interests pursued by the Data Controller, the client or *Expol,* except where such interests are overridden by the interests or fundamental rights of the data subject. Fraud prevention, cybersecurity and direct marketing are examples of the type of activities that might constitute legitimate interests.
   - ➢ **Vital interest –** The processing is necessary to protect the data subject's vital interests, such as in a medical emergency.
   - ➢ **Public interest –** Processing is necessary for a task carried out in the public interest.

2. **Purpose limitation –** Data processing must relate to a specific, explicit and legitimate purpose. Data must not be processed in a manner that is incompatible with the stated purpose/s. Generic purpose statements will not be compatible with the data protection legislation.

3. **Data minimisation –** Data collected must be limited to what is necessary. It must be adequate, relevant and not excessive, having regard to the stated purpose for which data is being processed.

4. **Accuracy –** Data must be kept accurate and up to date. Controllers must be able to correct personal data 'without undue delay.'

5. **Storage limitation –** Data should not be kept for longer than is necessary. Data retention policies should establish time limited for erasure, although it is permissible to retain data for longer periods of archive or statistical purposes only.

6. **Integrity and confidentiality –** Personal data must be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing, loss, destruction or damage, using appropriate technical or organisational measures.

Data Transfer

Expol's servers are based on the Isle of Man.

Data sharing

Expol do not share the personal data that is processed or collected by using this website with any third parties or use such data for any purposes other than what is outlined in this privacy policy. We do not sell your data.

A Reminder of your rights under GDPR

Data Subjects have the following rights regarding data processing:

- Right to information about processing
- Right of access
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restriction of processing
- Right to data portability
- Right to object to processing
- Rights with regard to automated processing and profiling

Expol

RISK MITIGATION & FORENSIC INVESTIGATIONS

If you have any questions or concerns about how your personal data is used, please contact the Data Protection Officer by email: enquiries@expol.co.uk.

Expol Ltd.
4th Floor, Hillary House
Prospect Hill, Douglas,
Isle of Man,
IM1 1EQ
Telephone: 01624 611190

Right to Complain

You can also make a complaint to the Information Commissioner, who is an independent regulator.

Isle of Man Information Commissioner
P.O. Box 69
Douglas
IM99 1EQ
Telephone: 01624 693260
Email: ask@inforights.im

This privacy notice may change from time to time. The date of its most recent update can be found at the top of this Notice.

End.