

## eSafeguarding privacy notice

### Welcome to eSafeguarding!

'We' are committed to protecting and respecting the privacy and security of your personal information.

### About us

In this Privacy Notice, references to 'we' 'us' or "our" means Protocol National Ltd t/a eSafeguarding. eSafeguarding is a company incorporated in England and Wales (registered number 3007851).

"our Group" includes Protocol, Protocol Assessment Services Ltd, and Teaching Force Ltd as well as our subsidiaries, our ultimate holding company and its subsidiaries as defined in section 1159 of the UK Companies Act 2006 and

"our websites" means [www.esafeguarding.co.uk](http://www.esafeguarding.co.uk)

### What is covered in this document?

This document explains how we collect and use personal information about you. For the purposes of this document "you" or "yours" refers to client or applicant users of the services provided by us.

"Service" or "services" means the service offered by eSafeguarding.

This notice together with our Cookie Policy sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us.

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a new regulation which replaces the Data Protection Regulation (Directive 95/46/EC). Even though the UK has expressed its intention to leave the EU in March 2019, the GDPR will be applicable in the UK from 25th May 2018. The Government intends for the GDPR to continue in UK law post Brexit and has also introduced a Data Protection Bill to replace the current Data Protection Act in due course.

Your new rights under the GDPR are set out in this notice but will only apply once the GDPR becomes law on 25th May 2018.

Please read the following, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal data about you, so that you are aware of how and why we are using your personal information.

For the purposes of data protection legislation in force from time to time the data controller is Protocol National Limited t/a eSafeguarding, of The Point, Welbeck Road, West Bridgford, Nottingham, NG2 7QW.

Our nominated representative is our Head of People & Performance. If you have any questions about your personal information, please email [data@protocol.co.uk](mailto:data@protocol.co.uk)

## Who we are and what we do

eSafeguarding is a DBS Registered Body and an umbrella body for the processing of DBS Criminal Record checks. Our service meets the requirements of the DBS in terms of how we collect, use and store your data. We provide our service via an online portal where clients, having first gained the consent of their DBS applicant will provide us with the personal data required to enable us to process your DBS check.

Our core business is the processing of online DBS checks for clients. DBS checks can only be requested by organisations who meet the DBS eligibility criteria. (the “Core Business”)

We collect information about you to carry out our Core Business.

## The personal information we collect, store and use

### 1 Information that you give to us

This is information about you that you give us by filling in forms on our website, in paper format or by communicating with us by phone, e-mail, text, post or otherwise.

It includes information you provide when you register to use any of our websites, to enter our database, to subscribe to our services, to attend our events, to participate in discussion boards or other social media functions on our websites, enter a competition, promotion or survey, and when you report a problem with any of our websites.

Depending on the nature of our relationship with you the information you give us or we collect about you may include your name; address history; private and corporate e-mail address; phone number(s); financial information such as bank account details (clients only); compliance documentation (DBS ID documents); age/date of birth; nationality; place of birth; gender/gender identity; and general correspondence.

### 2 Information we collect about you when you visit any of our websites

As well as any information you give to us by filling in forms on our websites, on each of your visits to any one of our websites we will automatically collect the following information:

- technical information, including the Internet protocol (IP) address used to connect your computer to the Internet, your login information if applicable, browser type and version, browser plug-in types and versions, operating system and platform;
- information about your visit, including the full Uniform Resource Locators (URL), clickstream to, through and from our site (including date and time), products you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), methods used to browse away from the page, and any phone number used to call the company.

### 3 Information we obtain from other sources

We may obtain personal information about you from other sources such as when your employer requests a DBS check which may include name and email address, list of identification documents seen in support of the application, staff numbers and or other unique identifiers.

We are working closely with third parties including companies within our Group, business partners, sub-contractors in technical, professional, payment and other services, external validation check providers, analytics providers, search information providers, credit reference agencies, professional advisors. We may receive information about you from them for the purposes of our Core Business.

## Purposes of the processing and the legal basis for the processing

We will only use your personal information when the law permits us to.

The majority of the processing of your data is performed by us for one of three reasons:

### 1) Necessary for contract

This means that we process your data in order to carry out our obligations arising from any contracts that we either intend to enter into or have entered into with you and to provide you with the information, products and services that you request from us.

### 2) Legal obligations

Certain processing of your personal data is required to enable us or your employer to meet legal obligations. For example, when you apply for work within a regulated activity you are obliged to undergo a DBS check.

### 3) Legitimate interests

In certain cases, we may process your personal data in order to further our legitimate business interests, or to help our clients to satisfy their legitimate interests. We will only do this when we have considered whether there is any other way to fulfil the relevant legitimate interest and balanced our legitimate interests against your right to privacy/the impact the processing has on your privacy.

An example of processing to fulfil a legitimate interest is our practice of recording all calls made to and by us. We state on our website and on calls that they are recorded. The recordings are held securely for a limited time and a very limited number of people have access to them. We use the recordings where there has been a complaint or dispute, to enable us to verify what was actually said. This is a mutual benefit to both you and us, as it helps facilitate fair resolution of any issues and helps to protect all parties from being subject to false accusations.

## Consent

We seek express applicant and candidate consent to the processing of your criminal record data and to the DBS providing an electronic result directly to eSafeguarding as the Registered Body which will be shared with your employer / requesting organisation.

In other cases, we may request consent by email, phone or by an online process for the specific activity we require consent for and record your response on our system. Where consent is the lawful basis for our processing you have the right to withdraw your consent to this particular processing at any time.

## Other Uses of your data:

- to notify you about changes to our service;
- to ensure that content from our site is presented in the most effective manner for you and for your computer.

We will use this information:

- to administer our site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
- to improve our site to ensure that content is presented in the most effective manner for you and for your computer;
- to allow you to participate in interactive features of our service, when you choose to do so;
- as part of our efforts to keep our site safe and secure;
- to measure or understand the effectiveness of advertising we serve to you and others, and to deliver relevant advertising to you (if applicable);
- to make suggestions and recommendations to you and other users of our site about goods or services that may interest you or them.

## Other information we collect

- **Social buttons.** On many of the pages of Our websites you will see 'social buttons'. These enable users to share or bookmark the web pages. There are buttons for: Twitter, Facebook and LinkedIn. In order to implement these buttons and connect them to the relevant social networks and external sites, there are scripts from domains outside of Our websites. You should be aware that these sites are likely to be collecting information about what you are doing all around the internet, including on our websites'. So, if you click on any of these buttons, these sites will be registering that action and may use that information. In some cases, these sites will be registering the fact that you are visiting Our websites, and the specific pages you are on, even if you don't click on the button if you are logged into their services, like Google and Facebook. You should check the respective policies of each of these sites to see how exactly they use your information and to find out how to opt out, or delete, such information.
- **External web services.** We use several external web services on the Our websites, mostly to display content within our web pages. For example, to display slideshows we sometimes use SlideShare; to show videos we use YouTube and Vimeo. This is not an exhaustive or complete list of the services we use, or might use in the future, when embedding content, but these are the most common. As with the social buttons we cannot prevent these sites, or

external domains, from collecting information on your usage of this embedded content. If you are not logged in to these external services then they will not know who you are but are likely to gather anonymous usage information e.g. number of views, plays, loads etc.

- **Email tracking.** Some emails that we send you have no tracking in at all, for example personal correspondence or emails with invoices attached. Other emails we send we put in tracking so that we can tell how much traffic those emails send to our site and we can track, at an individual level, whether the user has opened and clicked on the email. We rarely use the latter information at a personal level, rather we use it to understand open and click rates on our emails to try and improve them. Sometimes we do use the personal information e.g. to re-email people who didn't click the first time. If you want to be sure that none of your email activity is tracked, then you should unsubscribe from our email campaigns.

## Links to other websites

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over the other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

## Automated decision making

We do not undertake automated decision making or profiling. We do use our computer systems to search and identify personal data in accordance with parameters set by a person and / or a client. A person will always be involved in the decision making process.

## Cookies

Our website uses cookies to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and also allows us to improve our site. For detailed information on the cookies we use and the purposes for which we use them see our Cookie notice.

## Disclosure of your information inside and outside of the EEA

In the course of our Core Business we will share your personal information with:

- The DBS, your employer / requesting organisation.

We may also share client data with selected third parties including [we do not advertise services to individual users]:

- subcontractors including email marketing providers, payment and other financial service providers
- advertisers and advertising networks that require the data to select and serve relevant adverts to you and others. We do not disclose information about identifiable individuals to our advertisers, but we will provide them with aggregate information about how many candidates clicked on to their advert on our site.
- analytics and search engine providers that assist us in the improvement and optimisation of our site;

Other circumstances in which we may disclose your personal information to third parties are:

- In the event that the business or its assets were bought or sold or with a view to sale, we will disclose your personal data to the prospective seller or buyer of such business or assets.
- If we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply our terms and conditions of supply of services and other agreements; or to protect the rights, property, or safety of eSafeguarding, our customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

The lawful basis for the third party processing will include:

- their own legitimate business interests in processing your personal data, in most cases to fulfil their legal obligations;
- satisfaction of their contractual obligations to us as our data processor;
- for the purpose of a contract in place or in contemplation;
- to fulfil our legal obligations.

Whenever data is shared with third parties we require that the third party takes appropriate security measures to protect your personal information in line with our policies. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

## Where we store and process your personal data

The data that we collect from you is currently stored within the EEA. However in the future should your personal data be transferred outside the EEA or countries recognised by the European Commission as having an adequate data protection regime we will put in place appropriate measures to ensure that your personal information is held in those locations in a way that is consistent with and which respect the EU and UK laws on data protection, including one or more of the following binding corporate rules; use in contracts of standard data protection clauses approved by the European Commission.

## Data security

All information you provide to us is stored on our secure servers. Further we limit access to your personal information to those employees, agents, contractors or other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Any payment transactions will be encrypted using SSL technology. Where we have given you (or where you have chosen) a password which enables you to access certain parts of our site, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

## Retention of your data

We comply with the DBS Code of Practice on Secure Storage, Handling and Retention of data. We understand our legal duty to retain accurate data and only to retain personal data for as long as we need it to fulfil the purposes we collected it for. Accordingly, we have a data retention policy and run data routines to remove data in line with the policy. To determine the appropriate retention period for personal data we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, as well as the applicable legal requirements.

We may archive part or all of your personal data or retain it on our financial systems only, deleting all or part of it from our main Customer Relationship Manager (CRM) system. We may pseudonymise parts of your data, particularly following a request for suppression or deletion of your data, to ensure that we do not re-enter your personal data on to our database, unless requested to do so.

For your information, Pseudonymised Data is created by taking identifying fields within a database and replacing them with artificial identifiers, or pseudonyms. Our current retention policy is available upon request.

## Direct marketing to Clients

You have the right to ask us not to process your personal data for marketing purposes. We will always aim to inform you (before collecting your data) if we intend to use your data for such purposes or if we intend to disclose your information to any third party for such purposes and we will collect express consent from you if legally required prior to using your personal data for marketing purposes.

You can exercise your right to accept or prevent such processing by checking certain boxes on the forms we use to collect your data. You can also exercise the right at any time by unsubscribing from emails or contacting us at [info@esafeguarding.co.uk](mailto:info@esafeguarding.co.uk)

Our site may, from time to time, contain links to and from the websites of our partner networks, /partner service providers, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

## The GDPR provides you with the right to:

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object or withdraw your consent where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party in certain formats, if practicable.
- **Make a complaint** to a supervisory body which in the United Kingdom is the Information Commissioner's Office. The ICO can be contacted through this link: <https://ico.org.uk/concerns/>

## Access to information

The Data Protection Act 1998 and the GDPR give you the right to access information held about you. We also encourage you to contact us to ensure your data is accurate and complete.

Your right of access can be exercised in accordance with the Act (and the GDPR once it is in force). Prior to 25th May 2018 any access request under the Data Protection Act will be subject to a fee of £10 to meet our costs in providing you with details of the information we hold about you.

A subject access request should be submitted to [data@protocol.co.uk](mailto:data@protocol.co.uk) No fee will apply once the GDPR comes into force.

## Changes to our privacy notice

Any changes we make to our privacy notice in the future will be posted on this page and, where appropriate, notified to you by e-mail. Please check back frequently to see any updates or changes to our privacy notice.

## Contact

Questions, comments and requests regarding this privacy notice are welcomed and should be addressed to [data@protocol.co.uk](mailto:data@protocol.co.uk)