# REGISTER OF CHARTERED SECURITY PROFESSIONALS

**PRIVACY POLICY**

|  |  |
| --- | --- |
| **Owner: D Thomas** | **Date Created: 30th October 2018** |
| **Approved By: R Mounfield** | **Date Approved:** |
| **Document Ref:** | **Version 1** |

**Policy:** This document confirms how personal data is handled by the Register of Chartered Security Professionals (the Register) to ensure compliance with General Data Protection Regulations (GDPR) 2018.

**Purpose:** To ensure responsibilities are clear and to inform anyone wishing to engage with the Register about who has access to their personal data and what happens in order to protect it.

**Scope: This Privacy Policy is written and maintained by the Security Institute (the Agent) and managed by the Chartered Security Professionals Registration Authority (CSPRA) on behalf of the Register of Chartered Security Professionals (the Register) and the Worshipful Company of Security Professionals (the Company). It applies to any person or organisation involved in handling personal data on behalf of the Register.**

1. **Introduction**

**The Security Institute promises to respect and look after all personal data shared with us, or that we get from other organisations. We will always keep it safe. We aim to be clear when we collect your data about what we’ll use it for, and not to do anything you wouldn’t reasonably expect. We will never sell your personal data to other organisations and will only ever share it in appropriate, legal or exceptional circumstances.**

1. **Responsibilities**

The Company owns the Register and has appointed an Agent to develop and manage the Register on its behalf, whilst the Company retains overall responsibility for it. CSPRA is a sub-committee of the Company and is responsible to the Company. It has delegated authority (although not responsibility) to govern all aspects of the Register.

CSPRA licenses suitable professional bodies (the Licensees) to admit qualified applicants to, and to remove them from, the Register. CSPRA is also responsible for setting and maintaining standards of professional competence, code of professional ethics and a disciplinary code, and resolving any appeals or complaints against registrants.

Although several different organisations may collect, use and retain your personal data, they are all governed by CSPRA and this Privacy Policy.

1. **Data Collection**

We collect information in the following ways:

**3.1 When you give it to us DIRECTLY** such as when you enquire about coming a CSyP, or apply to be admitted, or by attending one of our events or engage in opportunities we notify you about. Sometimes when you engage with us, your information is collected by an organisation working for us (eg a sponsorship consultant or charity) or an individual trying to mentor/encourage you, but we remain responsible for your data at all times.

**3.2 When you give it to us INDIRECTLY** such as when your information is shared with us by independent event organisers or learning providers, for example University or training student memberships, or trade shows such as SCTX, IFSEC or International Security Expo. These independent third parties will only do this if you have indicated that you are happy for them to do so. You should check their Privacy Policy when you provide your information, to understand in full how they will process your data. Dependant on your settings or the privacy policies for social media and messaging services that we use, such as Facebook, Twitter, Instagram or Linked In, you might give us permission to access information from those accounts or services. The information we get from other organisations may depend on your privacy settings or the responses you give, so you should regularly check them.

**3.3 When it is PUBLICLY AVAILABLE** which may include information found in places such as Companies House and information that has been published in articles either printed or online. We may combine information you provide to us with information available from external sources in order to gain a better understanding of our applicants.

**3.4 When we collect it as you use our WEBSITE OR APP** like most websites, we use “cookies” to help us make our website and the way you use it better. Cookies mean that a website will remember you. They are small text files that sites transfer to your computer (or phone or tablet). They make interacting with a website faster and easier- eg by automatically filling your name and address into text fields. As well as this, cookies can tell us the type of device you are using to access our website or apps and the settings on that device may provide us with information including what type of device it is, what operating system you are using, what your device settings are and why a crash has happened. This information helps us understand how people are using our website or mailing system, and shows us how to make it better. Your device manufacturer or operating system provider will have more details about what information your device makes available

1. **What information is collected?**

The type and quantity of information we collect depends on why you are providing it. If you are a CSyP, for example, when you log into web services, purchase event tickets or request mentoring partnerships, we will usually collect:

* Your name
* Your contact details

Where it is appropriate, we may collect:

* Information about the service you are requesting
* Your payment details
* Your employment details
* Your qualifications details
* Your vetting status

We will only ever ask for information that is needed to host an event, provide the services you have requested, provide pertinent information bulletins or administer the CSyP admittance or retention service you have requested.

When applying for admission to the Register, a detailed list of your personal data will be collected. This is necessary to ensure that all CSyP applicants can be screened (BS7858), reference checks conducted and evidence gathered prior to submission to the Document Assessment Panel and Professional Interviewers for their review, and a final recommendation for admittance to be made to the Registrar for a decision to admit or refer the applicant. We collect:

* Gender
* Full name
* Date of Birth
* Payment method ( DD or annual payment)
* Qualifications and training
* Employer and address
* Job title
* Home address
* Preferred contact details ( email and telephone)
* Details of work experience and commitment and contribution to professionalism
* Prior Conduct information
* Photo
* Opt In information for future marketing mailings
1. **How we use the personal data we collect**

What we use your information for depends on the reason you are providing it. The information we collect in order to provide these services may be sensitive relating to employment or skill sets that you do not wish to be known. We will mainly use your data to:

**5.1 Provide you with the application service to be admitted as a CSyP.** Your information will be shared with vetted assessors involved in the admittance process. Access to this data will always be limited to appropriate individuals with a legitimate interest in supporting your application. All members of the assessment panels are themselves CSyPs, and therefore bound by the Code of Professional Conduct.

Once the application process has completed, your file will include copies of all relevant correspondence including Document Assessment Reports, Professional Interview Reports, reference responses and Final Assessment comments.

If your application to be admitted is unsuccessful and you subsequently appeal that decision, your information will be shared with members of the appeal panel headed by the Chairman of CSPRA.

**5.2** **Remaining on the Register.** Each year CSyPs are required to successfully participate in the Security Institute Continuous Professional Development (CPD) scheme. Reminders are issued, records of activity verified and a Certificate of Completion issued. In addition, annual renewal fees must be paid.

**5.3** **Confirm your admittance to the Register to the public**. A list of all CSyPs (name, employer, location) is published on [www.charteredsecurityprofessionals.org](http://www.charteredsecurityprofessionals.org) and [www.security-institute.org](http://www.security-institute.org) . This is the public Register of Chartered Security Professionals. You may Opt Out of being listed. The Company receives contact and employment details of all CSyPs.

**5.4 Direct Marketing** We will only ever contact you with direct marketing about the Register, events and campaigns with your explicit consent. You do this on your application form when you first apply. If you change your mind at any time, and no longer wish to hear from us, just let us know when you provide your data, contact us on info@charteredsecurityprofesional.org We do not sell or share personal details to third parties for the purposes of marketing. Occasionally, we may include information in our communications from partner organisations or organisations who support our aims.

You have the option at any time to change your mind and to OPT OUT of receiving global email. You will only then receive information directly relevant to you remaining on the Register of Chartered Security Professionals, such as CPD and annual fee reminders.

**5.5 Continuous improvement and ongoing engagement**. Developing a better understanding of our supporters/ CSyP through their personal data means we can make better decisions, organise CPD events more efficiently and ultimately, helps us to reach our goal of promoting professionalism amongst CSyPs and the wider security industry.

We may collect and retain your information if you provide feedback about our services, give a compliment or make a complaint. We do this in order to improve our service, information and events. We believe it is important to make sure our communications, opportunities and networking initiatives are the best they can be. That is why we evaluate them and may get in touch to get your views on your experience. There is no obligation to take part, but it really helps to highlight ways we can make things better in the future.

We record communication preferences so that we only contact you in the ways you wish to hear from us. We don’t want to waste your time or send global communications that you do not value. We consider belonging to the Register as constituting legitimate interest.

We may analyse geographic, demographic and other information relating to you in order to better understand your interests and preferences in order to contact you with the most relevant communications including events, employment opportunities and engagement opportunities (such as presenting) with us, based on your skills and expertise. We do this because it allows us to understand the background and specialist skills of CSyPs and helps us to find volunteers and future event hosts, and to raise the profile of the Register.

Some CSyPs choose to tell us about their experiences or employment field for the benefit of the wider security sector including potential CSyPs. This might include information about past operations, advisory notes or failures, news articles, together with photos and/or video. We will always ensure we have explicit and informed consent from the individuals involved. We will always keep this information safe and secure. This information may be shared at events, in promotional materials (newsletter/e-News) or professional development workshops.

1. **Sharing your data**

We do not share or sell personal details with third parties for the purposes of marketing.

Once admitted your name, company, country of residence and date of admittance will be published on the web-based Register of Chartered Security Professionals. You will have the opportunity to opt out of this prior to your details being published.

We will only share your details with third party organisations when it is necessary to;

6.1 Provide you with the services you have asked for – we will make sure you are happy for us to do this before anything happens and will explain who we are sharing the data with e.g. mentors, government agencies, recruiters, etc.

6.2 Administer your participation in an event or CPD activity.

6.3 Comply with health and safety regulation.

If we ever need to share data for these purposes, we will always take the utmost care, ensuring only essential data is transferred and that it is done so safely and securely.

**Exceptional circumstances**

We may be required to share your details in exceptional circumstances. For example, to comply with a professional code of conduct, where required by the Police, regulatory bodies, or legal advisors.

We will only ever share your data in other circumstances if we have your explicit and informed consent.

1. **How we keep your data safe and who has access**

We ensure there are appropriate measures and controls in place to protect your personal details. Access to files on our network is protected and routinely monitored, and 3rd party file sharing (used during assessments) is minimised and personalised. We undertake regular reviews of who has access to information that we hold, to make sure that your information is only accessible to appropriately trained staff and partners.

Before we use any external companies to collect or process personal data on our behalf, such as collection of annual CPD records or renewal fees, we will complete comprehensive checks. We will always put a contract in place that sets out our expectations and requirements, especially how they manage the personal data they have collected or have access to.

Suppliers who run their operations outside the European Economic Area (EEA) are not subject to the same data protection laws as companies based in the UK. However, if we ever choose to use a supplier based outside the EEA, we will make sure that they provide an adequate level of protection in accordance with UK data protection law.

1. **Keeping your information up to date**

We try and keep our records up to date so that we can send you the most relevant information. You should ensure we have the correct contact details for you, particulary regarding CPD records. If you change employment, please update your contact details as soon as its practical.

Where possible we use other members or publicly available online resources (LinkedIn, Twitter or past employers) to trace your new contact details if we lose contact with you. This is to ensure that your intention was to leave the Register and not an administrative oversight. If you do wish to leave the Register, please inform us and your personal details will be deleted from our database.

Application records are retained for the duration of the time you remain on the Register in order to internally handle any issues concerning appointment, competence and complaints. Files will be retained for 24 months after you leave the Register or fail to be admitted, in case of return or re-application.

1. **Your “right to know” what we know about you, make changes or ask us to stop using your data.**

You have the right to ask us to stop processing your personal data. If you do this, then we will have no option but to cancel your registration as a Chartered Security Professional.

You have the right to ask for a copy of the information we hold about you. If there are any discrepancies in the information we provide, please let us know and we will correct them.

If you want to access your information, send a description of the information you want to see and proof of your identity by post to the Data Controller, The Security Institute, 1 The Courtyard, Caldecote, Warwickshire, CV10 0AS. We do not accept these requests by email. This is a security measure to ensure we do not provide your information to an unentitled person.

If you have any questions relating to this policy please email info@charteredsecurityprofessional.org For further information, see the Information Commissioner’s guidance at ( www.ico.org.uk).

1. **Changes to the Policy**

We review this policy annually and may update it from time to time. If we make any significant changes in the way we treat your personal information, we will make this clear on our website or by contacting you directly.