

DATA PROTECTION & PRIVACY NOTICE

Concerto IP Limited (trading as Concerto IP), is a company registered in England & Wales under Registration Number 9504319.

We are an intellectual property law practice regulated in the United Kingdom by the Intellectual Property Regulation Board (IPReg).

Our trading address (for correspondence by post) is Enterprise Hub, Kao Hockham Building, Edinburgh Way, Harlow, Essex CM20 2NG, United Kingdom. Tel +44 (0)1277 896049.

Our registered address with effect from June 11, 2018 is Kingfisher House, 11 Hoffmann's Way, Chelmsford, Essex CM1 1GU, United Kingdom.

The person responsible for data protection compliance in our business is Malcolm Lawrence (malcolm@concerto-iplaw.com Telephone +44 (0) 1277 896313).

Concerto IP Limited Data Protection & Privacy Notice

Our data protection principles

We will comply with data protection law

The personal information we hold will be:

Used lawfully, fairly and in a transparent way

Collected only for valid purposes that we have clearly explained and not used in any way that is incompatible with those purposes

Relevant to the purposes we have disclosed and limited to those purposes

Accurate and kept up to date

Kept only for as long as necessary for the purposes we have disclosed

Kept securely, and shared carefully if sharing is necessary

1. What this Notice is about

This Notice is to provide you with the following information about our compliance with data protection legislation, and GDPR¹ in particular:

- 1.1. Notice that we collect, hold, use and sometimes share personal information - in other words we *process* it².
- 1.2. The purposes for which we process it.
- 1.3. Who the information is processed about (who are the data subjects).
- 1.4. The types of personal information we process.
- 1.5. How we collect personal information.
- 1.6. Our website.
- 1.7. The lawful basis for our processing of personal information.
- 1.8. Sharing personal information – when and how we do this.
- 1.9. Storage - How we safeguard personal information to protect the privacy of the data subject.
- 1.10. The rights of data subjects in relation to the information we process

2. Notice that we process *personal information and are subject to GDPR*

- 2.1 We process personal information by collecting, storing, using and sometimes sharing it.
- 2.2 By personal information, we mean “*any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier*”.
- 2.3 Personal information includes basic information such as a person’s name and business and personal email addresses plus other contact details, but it also covers, less obviously, information such as identification numbers, electronic location data and online identifiers.
- 2.4 We only process personal information for a purpose we record in our systems together with a note of the lawful basis for the processing.

¹ The General Data Protection Regulation – Regulation (EU) 2016/679

² Data protection legislation uses a number of terms (such as *processing*) which have a legal definition. You may want to look up these definitions by navigating to <https://gdpr-info.eu/art-4-gdpr/>.

- 2.5 Our processing of personal information is expressly limited to the purpose for which we collected it. We stop processing it for that purpose when the purpose or the lawful basis for the processing ceases to exist.
- 2.6 We have a legal obligation to safeguard any personal information we store. Our professional business is about product, process and business ideas - confidential information with commercial value - and so safeguarding information is something where we are experienced.

3. The purposes for which we process personal information

- 3.1. We process personal information primarily to enable us to provide legal services relating to intellectual property in performance of contracts entered into between Clients and ourselves and to enter into those contracts.
- 3.2. We also process personal information to:
 - 3.2.1. Maintain the records required to provide our services and manage our finances and other aspects of our business.
 - 3.2.2. Comply with the code of conduct set down by our Regulator, IPReg (including, in that it applies to us, the code of conduct for litigators regulated by that Regulator).
 - 3.2.3. Comply with anti-money laundering legislation and any other legal obligation which requires us to process the personal information concerned.
 - 3.2.4. Enable us to demonstrate our compliance with GDPR and any other data protection legislation to which we are subject.
 - 3.2.5. Enable us to uphold the rights of employees and our rights as employers, and to assess applications for employment, offers for the supply of goods and services and the credit status of any person with whom we are considering the transaction of business;
 - 3.2.6. Enable us to defend any claims made against us, and any complaints made about us; and
 - 3.2.7. Enable us to prepare and prosecute, or settle, any claims we have against another person and any complaints we have about any other person.

4. Who the information is processed about (who are the *data subjects*)

- 4.4. We process personal information about data subjects in the following categories:
 - 4.4.1. Clients, and Client Employees (whether under contract of employment or not)
 - 4.4.2. Colleagues in the intellectual property profession - IP professionals:
 - as actual or potential instructors of our business
 - as actual or potential IP service suppliers.
 - 4.4.3. Other suppliers and potential suppliers
 - Including advisers, consultants, experts and professional service providers other than IP professionals.
 - 4.4.4. Other Business Contacts.
 - 4.4.5. Enquirers not included in any of the above categories.
 - 4.4.6. Special categories:
 - Employees
 - Prospective employees.

5. The types of personal information we process

- 5.1. We process information which is relevant to the purposes set out in Paragraph 3.
- 5.2. This information may include:
 - 5.2.1. Personal details such as:
 - Name
 - Date of Birth
 - Gender

- Physical address
 - Email address
 - Telephone number(s)
 - Job title
 - Job responsibilities
 - Profession
 - Bank details
 - Education, employment and career detail
 - Information contained in documents provided for compliance with the anti-money laundering requirements of our Regulator insofar as not mentioned in the list above.
- 5.2.2. Special classes of sensitive information that may include:
- Information which the data subject regards as confidential
 - Information which the data subject regards as sensitive
 - Rarely, physical or mental health details.
- 5.3. We would rarely process for any single individual all the personal details listed in Paragraph 5.2.1.

6. How we collect personal information – data subject categories

We collect information in a number of ways. Some apply to all the categories of data subject, whilst others apply only to some but not all of them. It is unlikely that all methods of collection would be employed for any particular person.

6.1. Collection methods used generally

The following sources for a person's personal information are methods we use, and have used, for data subjects in general, although it is unlikely that all would be employed for any particular person:

- 6.1.1. The person himself or herself.
- 6.1.2. Publicly available sources.
- 6.1.3. The membership list of a society or similar organ which it made available to a staff member of our company.
- 6.1.4. The person's listed or actual attendance at a conference or business networking event at which a staff member of our company was also a listed or actual attendee.
- 6.1.5. Personal introduction to a staff member of our company including, for example, introduction at or in connection with an event to whose organiser a fee was paid for introductions and at which event the person was invited to be a delegate or sponsor.
- 6.1.6. The person's LinkedIn profile if they gave access to it to a staff member of our company by linking with them in that social media system at their invitation or ours.
- 6.1.7. If the person was previously a data subject in another category and we still hold personal information about them in that capacity, that personal information but subject to our updating it to reflect the change in their capacity.
- 6.1.8. Another information source which has been divulged to the data subject in writing.

6.2. Collection in the case of Clients and Client Employees

If you are or have ever been our Client or a Client Employee, the personal information sources listed below, and the examples listed below of sources indicated in Paragraph 6.1, may be used (and may have been used) for personal information collection:

- 6.2.1. Information you provide to us through your opting-in to receive our IP Education Materials³.

³ For emailing list purposes, we collect and store only your email address, personal name, firm name and country. Where, in the past, we have collected more information for this purpose (eg full address and telephone

- 6.2.2. Publicly available “official” sources:
 - o Bodies of information kept by intellectual property offices and available to the public free of charge or on payment of a fee
 - o Bodies of information kept by a commercial third party and based on the above sources.
- 6.2.3. Someone providing it for you and authorised to do so, such as
 - o The Client, if at the time of collection, you were a Client Employee of that Client, or
 - o A professional acting for you or (if at the time of collection, you were a Client Employee of that Client) for that Client.

6.3. Collection in the case of Colleagues - IP professionals

If you are Colleague, the personal information sources listed below, and the examples listed below of sources indicated in Paragraph 6.1, may be used (and may have been used) for personal information collection:

- 6.3.1. If you are a Colleague not in private practice in the territory represented by the member states of the European Patent Convention⁴, information provided by your engagement with us pursuant to our sending to you European Law & Practice-related information⁵ likely to be of value to that sub-category of Colleague as a class.
- 6.3.2. The following publicly available sources:
 - o The internet
 - o The website of the firm where you practice (if you are in private practise)
 - o A law & practice publication for which you are an author
 - o The membership list of a society or similar organ which is publicly available.
- 6.3.3. Professional correspondence between us concerning the business affairs of a mutual Client or respective Clients

6.4. Collection in the case of other business contacts and enquirers

If you are not a Client or Colleague, the personal information sources listed below, and the examples listed below of sources indicated in Paragraph 6.1, may be used (and may have been used) for personal information collection:

- 6.4.1. Information you provide to us through your opting-in to receive our IP Education Materials⁶.
- 6.4.2. The following publicly available sources:
 - o The internet
 - o The website of the business in which you work
 - o The membership list of a society or similar organ which is publicly available.

6.5. Collection in the case of employees and prospective employees

In relation to employees and prospective employees, personal information is collected from the following sources:

Employees	Directly from the employee and, with their consent, from any other source and always subject to the conditions of the consent
-----------	---

numbers), we have started an internal process to remove this additional information in line with the GDPR principle of collecting only the minimum personal information required to fulfil our purpose

⁴ For example, (i) an in-house patent attorney in practice in one of the above locations in the patent department of a company which has an interest in patents as an owner or licensee or (ii) an intellectual property professional in private practice in the USA. These are examples of persons we judge are likely to benefit from European Law & Practice information and opinion we can provide.

⁵ See Footnote 3

⁶ See Footnote 3

Prospective employees	Directly from the prospective employee and, with their consent, from any other source and always subject to the conditions of the consent
-----------------------	---

7. Our website

- 7.1.** Google, as our website analytics service provider, collects personal information, in the form of cookies, whenever someone accesses it, and this is stored by Google. If you register for access to the gated part of our website, you will in doing so disclose to us personal information which is stored by us in a database on our website.
- 7.2.** Personal information in the form of cookies may be used by us to inform web site changes which from time to time we make, or have made by others, to improve the performance of our website.
- 7.3.** We do not carry out any process, and no process is carried out for us by any other party, to refine any of the personal information referred to in Paragraphs 7.1 and 7.2 to identify more precisely any person whose personal information is included in the information collected.

8. The lawful basis for our processing of personal information

The lawful basis for our processing of personal information depends on which of the categories set out in Paragraph 4 is one in which the data subject concerned falls. This is principally because our relationships with data subjects differ from category to category.

8.1. Clients and Client Employees when there is a Client contract

The lawful basis on which we process personal information is (i) our legitimate interests relating to the performance of contracts between us and Clients who have instructed us and (ii) the legitimate interests of those Clients.

8.2. Clients and Client Employees who have opted-in to our IP Education Materials

The lawful basis on which we process personal information is (i) those Clients and Client Employees having opted-in to receive our IP Education Materials and/or (ii) our legitimate interests in educating clients and their legitimate interests in IP education to assist them in managing their IP affairs.

8.3. Colleagues

The lawful basis on which we process personal information is as follows:

- 8.3.1.** In the case of Colleagues in private practice in the territory represented by the member states of the European Patent Convention⁷ and who have opted-in to receiving our UK Law & Practice-related information: the consent of those Colleagues
- 8.3.2.** In the case of Colleagues not in private practice in the territory represented by the member states of the European Patent Convention⁸: (i) our legitimate interests in disseminating, as an information service, significant European law & practice information and opinion likely to be of value to that sub-category of Colleagues as a class and (ii) the legitimate interests of those recipients to keep updated on European law & practice in the interests of the clients they represent⁹.

8.4. Suppliers of goods and services (and potential suppliers)

The lawful basis on which we process personal information is our legitimate interests in managing our business transactions with the suppliers and gathering information from them and potential suppliers to inform our procurement decisions.

8.5. Enquirers, employees and prospective employees

⁷ This area is shown on the [attached map](#) (copyright European Patent Organisation)

⁸ Examples of such Colleagues are (i) an in-house patent attorney in practice in one of the above locations in the patent department of a company which has an interest in patents as an owner or licensee or (ii) an intellectual property professional in private practice in the USA

⁹ We judge that Colleagues in this sub-category are likely to benefit from European Law & Practice information and opinion we can provide as an information service and/or from an exchange of broader law and practice information and/or IP industry information between us.

The lawful basis on which we process personal information is as follows:

Enquirers about our services	Our legitimate interest in professionally responding to the enquiry concerned, including allowing a period for further enquiry before deleting the personal information (unless we judge that we should keep it longer in order to defend ourselves against any claim made against us or complaint made to us or about us)
Employees	The consent of the employee to the processing
Prospective employees	The consent of the prospective employee to the processing

9. Sharing of personal information

- 9.1. Whether sharing any of a person's personal information with any third party becomes necessary in practice depends a great deal on the person's data subject category (see Paragraph 4). For the most part, we share little personal information with any third party.
- 9.2. However, in addition to sharing with the individual his/her own personal information we process, we sometimes need to share it with others, eg organisations other than ourselves. Where such sharing of the personal information we process is necessary we are required to comply with all aspects of the Data Protection Act (DPA)¹⁰:
- 9.3.1. Where the sharing of personal information is reasonable and to be expected, we would not normally require your consent. However, where this is not so, we will first request your informed consent and share the information only when we have obtained that consent.
- 8.3.1 We will never share a person's sensitive or confidential personal information with any third party without your written informed consent unless doing so is the only practical way of protecting a vital interest of the person or another party (eg a life is in danger).
- 8.3.2 Under our current policies, we will not share personal information with any third party for the purposes of assembling marketing or profiling information. We will never sell personal information; in particular, we will not sell personal information collected through use of our website.
- 8.3.3 Over-riding all of the above, we would always share personal information if ordered to do so by a court or regulatory body having the jurisdiction to do so. However, this is very rare.
- 9.3. The reasons for information sharing vary. For example, as occurs in our business, a patent application may require the filing of a declaration giving the names and contact details of the inventors of the invention concerned, this being a formal legal requirement which must be satisfied for the patent application to proceed.
- 9.4. The following is a description of the principle types of organisations with whom we may need to share some of the personal information we process:
- 9.4.1. Intellectual property offices such as the UK Intellectual Property Office (primarily Newport, Wales), the European Union Intellectual Property Office (Alicante, Spain), the European Patent Office (primarily Munich, Germany) and the World Intellectual Property Organisation (Office of the PCT) (Geneva, Switzerland)
- 9.4.2. Persons and firms having rights of legal representation (eg in jurisdictions outside the EU) necessary to represent our Clients before authorities, courts and tribunals before which we do not have such representation rights.
- 9.4.3. Persons or firms having expertise or capacities which it is necessary to make available to our Clients, or otherwise in their best interests to make available to

¹⁰ Information from the Information Commissioner's Office on information sharing can be found [HERE](#)

them, in connection with legal services we are contracted to provide to them or in relation to which the Client has made enquiries of us.

- 9.4.4. Personal information we share with intellectual property offices will be limited to (i) that which it is formally required that we share to satisfy legal requirements which apply to intellectual property procedures concerning Client interests and (ii) that which is needed to support that Client's case. In case (i), this is normally confined to names, addresses and employment status. In case (ii), the information given may be more extensive and could involve sensitive personal information¹¹. It is important to understand that, in performance of its official functions, many intellectual property offices will, normally, make available to the public all information which we share with it at some point (which may be as soon as eg 14 days later). We have refined our processes for obtaining informed consent before personal information is shared which we could reasonably expect the data subject not to have realised would be published by someone who is allowed to share it.
- 9.4.5. In addition to the organisations listed in Paragraph 9.4, we may also need to share some of the personal information we process with other parties, but we will only do this if (and to the extent) (i) it is to be expected and is reasonable or necessary or (ii) we have your consent.

10. Storage and Security of Information

10.1. How we store information

- 10.1.1. We safeguard personal information and protect it from loss, damage, misuse, unauthorized third-party access, disclosure, alteration and destruction by measures we also use to protect Client confidential information such as technology and stock price-sensitive information. These measures in particular comprise:
- A desk clear policy when receiving visitors
 - End point protection for our IT equipment (including anti-virus protection, email and web surveillance, program behaviour shield, software firewall protection of computer terminals, and hardware perimeter firewall protection if this form of firewall should appear necessary on the basis of professional advice)
 - Separate malware protection
 - Password security for end point devices (including mobile devices) and a policy on their creation, use and accessibility
 - Guided by SRA recommendations, cloud storage of confidential information, which is:
 - backed up in real time or at least once in each period of approximately 24 hours
 - stored at secure Tier 3 service provider data centres in the United States, which have been compliant, since prior to commencement of GDPR, with the EU-US and US-Switzerland [Privacy Shield Framework](#)¹² and, more generally, with GDPR
 - protected by end-to-end encryption and encryption-at-rest
 - subject to a zero-knowledge encryption key policy (ie the encryption key is known only to us)
 - Staff vigilance for electronic threats in incoming electronic information

¹¹ For example, the health of a person may result in his not being able to comply with a legal deadline in intellectual property proceedings, in which case we may need to disclose his health to a patent office as justification for extending the legal deadline

¹² The EU-US framework was designed by the US Department of Commerce and the European Commission to provide companies engaged in US-Europe commerce with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the USA.

- Restricted individual employee rights to install new or updated software to our systems.
- 10.1.2. We will only hold personal information for so long as we need it to fulfil the relevant purpose(s), eg to demonstrate our compliance with data protection laws or to concord it with a request of its owner placing a limit or prohibition on its processing. However, whilst this may mean holding some personal information for the life of an intellectual property asset (a UK patent, for example, lasts for 20 years and is renewed annually), we will not hold information that is not necessary and will not hold it any for longer than need be.

10.2.Storage of personal information by a third party with whom we have shared it

- 10.2.1. In cases where we share information with one or more third parties who store information outside the EU/EEA, we take steps to satisfy ourselves that their data protection policies are in line with the regulatory requirements of GDPR and with our own data protection standards, and ideally that they participate in the EU-U.S. Privacy Shield Framework¹³ or a similar certification framework.
- 10.2.2. In our business, sharing information where it is stored outside the EU/EEA is most likely to arise where we cooperate with another party¹⁴ to provide a Client with a service. In most such cases, because the partner with whom we cooperate is most likely to be located in the EU/EEA or an advanced non-EU/EEA economy, it can generally be expected to have adopted responsible data protection policies.
- 10.2.3. However, this is not so for all countries¹⁵. For example, intellectual property services are sometimes provided on Client instructions for emergent economies, where data protection legislation may not exist in any modern form and which are not considered to provide adequate data protection.
- 10.2.4. Sharing by cross-border data transfer may, however, lawfully take place if the transfer is “*necessary for the establishment, exercise or defence of legal claims*”¹⁶. However, in any case where strict necessity is in doubt, the fully informed consent of the data subject¹⁷ in question (eg an expert witness whose testimony is to be relied upon in a contentious IP matter) must instead be obtained. We have changed our internal processes to ensure this is discussed between us and the parties concerned in the uncommon case where sharing outside of approved data protection frameworks may be contemplated.

10.3.How long we hold personal information

- 10.3.1. As with other professionals, we are required by our insurers to keep information relevant to any claims against us for as long as it may be required to defend any claim, whether for alleged breach of contract or alleged failure to discharge a duty of care arising outside of a contract.

¹³ The EU-US and Swiss-US [Privacy Shield Frameworks](#) were designed by the US Department of Commerce, the European Commission and Swiss Administration to provide companies engaged in transatlantic commerce with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the USA.

¹⁴ See Paragraph 9.4.2

¹⁵ Countries outside the EU/EEA considered to provide adequate data protection are noted on the EU website ([here](#)). In short, the European Commission has so far (as at May 21, 2018) recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate data protection.

¹⁶ Recital.111; Art.49(1)(e)

¹⁷ Recital.111; Art.49(1)(a)

10.3.2. The Table [HERE](#) provides further information about our policies in the above respects.

11. Rights of data subjects in relation to the information we process

- 11.1. All data subjects have the right to make a request (“*subject access request*”) to us to provide details of personal information we hold about themselves. That right includes the right to ask for a copy. The subject access request must be in writing and we ask that any subject access request be sent by email to malcolm@concerto-iplaw.com or by post to our office address (see page 1) marked “*Confidential request about my personal information you may keep*”.
- 11.2. We will usually reply to a subject access request free of charge. If the unusual circumstances in which GDPR states that a charge can be made apply, then we may make a lawful charge to recover administrative costs; but our aim is not to do this and we will never make a charge without first telling the data subject what it is.
- 11.3. We aim to respond to most subject access requests within 7 days of receipt and we will never take more than a calendar month except in the case of a complex request, where GDPR permits up to 3 months (in which case, we will keep the data subject informed). Any copies we provide will, if in electronic form, be in one of the convenient forms normally used for documents (eg Word, PDF).
- 11.4. A data subject may also wish to contact us by telephone (see page 1), although any subject access request must, as we have stated above, be in writing.
- 11.5. Data subjects have the right to ask us to stop processing their personal information (for a particular purpose or more generally), to delete it or disclose how it is used or shared. We will comply with such a request unless there is a lawful basis to decline it wholly or partially (eg we could decline to delete personal information because we need to keep a record of it to ensure that we do not inadvertently collect that personal information again and use it – other reasons why we may decline it wholly or partially will be evident from Paragraph 3).
- 11.6. Data subjects have the unconditional right (i) to opt-out of any service we provide by which we send them any kind of material (eg a newsletter) and (ii) to ask us to remove their contact details from our mailing and emailing lists. We have an obligation to comply with such a request, and to do so within a reasonable time.

12. Other matters

- 12.2. We have applied voluntarily for registration with the Information Commissioner’s Office.
- 12.3. We will produce a summary version of this document and publish it as soon as possible.

13. Changes to this Privacy Policy and Notice

- 13.2. We may change this Privacy Policy and Notice at any time, for example due to a change in the law, a change in best practice or a change in the types of personal information we process or how we process it.
- 13.3. Any such changes will be notified on our website and in our email footer.