Privacy Statement for Invicro

In July 2020, the Court of Justice of the European Union handed down ruling C-311/18 with respect to the adequacy of the mechanisms and safeguards in place in the USA to protect the data privacy rights of EU citizens. The legal structures – Privacy Shield and Standard Contractual Clauses (SCC) which had, prior to this judgement, been accepted as protecting these rights, were invalidated, and are now deemed insufficient protection for the data rights of EU citizens.

Any personal data transferred from the EU to the US may be accessed by the US government under the Foreign Intelligence Surveillance Act (2008), if such data is deemed to be relevant to the national security of the USA. This results in limitations to the protection of personal data which are not consistent with the laws of the EU.

The Company seeks to minimize the data that is transferred to the US, and your data will not be transferred without your consent. Data transferred to the US prior to ruling C-311/18 is not subject to this ruling and may be retained in the US unless you request its deletion.

Questions or concerns from individuals or entities located within the European Union should be addressed to enquiries@invicro.co.uk.

Invicro is a niche imaging Contract Research Organization (CRO) providing imaging services to clinical trials from translational drug discovery and development through to late phase clinical studies. To this effort, we offer a suite of services including the conduct and sponsorship of imaging clinical studies involving healthy volunteers and patients.

This Privacy Statement explains how and why we collect, process and retain information about research participants, clients and collaborators, and users of this website. Invicro is the data controller for the use of personal data in this privacy notice, with the exception of research data for studies where Invicro is not the Sponsor, in which case Invicro acts as the data processor.

The content of this policy covers the following:

Effective: July 2020
Last Updated: 30 July 2020

Privacy Shield

Invicro is strongly committed to protecting the privacy of those who entrust us with their personal information. Invicro complies with the EU-U.S. and the Swiss-U.S. Privacy Shield Frameworks, as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and/or Switzerland to the United States. Invicro has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal information from the European Union and Switzerland to the United States in support of transatlantic commerce. On July 12, 2016, the European Commission deemed the EU-U.S. Privacy Shield Framework adequate to enable data transfers under EU law (see the adequacy determination). On January 12, 2017, the Swiss Government announced the approval of the Swiss-U.S. Privacy Shield Framework as a valid legal mechanism to comply with Swiss requirements when transferring personal information from Switzerland to the United States. See the statements from the Swiss Federal Council and Swiss Federal Data Protection and Information Commissioner.

The Privacy Shield program, which is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce, enables U.S.-based organizations to join one or both of the Privacy Shield Frameworks in order to benefit from the adequacy determinations. To join either Privacy Shield Framework, a U.S.-based organization will be required to self-certify to the Department of Commerce and publicly commit to comply with the Framework's requirements. While joining the Privacy Shield is voluntary, once an eligible organization makes the public commitment to comply with the Framework's requirements, the commitment will become enforceable under U.S. law. All organizations interested

in self-certifying to the EU-U.S. Privacy Shield Framework or Swiss-U.S. Privacy Shield Framework should review the requirements in their entirety.

Definitions of Personal Information

"Personal Information" means information that can directly or indirectly lead to the identification of a living person, such as an individual's name, address, e-mail, telephone number, license number, medical identification number, photograph, or other identifying characteristic. The identification can occur by reference to one or more factors specific to the individual's physical, physiological, mental, economic, cultural or social identity. Personal information does not include information that has been anonymized, encoded or otherwise stripped of its identifiers, or information that is publicly available, unless combined with other non-public personal information.

“Sensitive Information” means Personal Information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life or sexual orientation of the individual.

Research Data

Invicro uses personally identifiable information to conduct research to improve health and care. As a research company we have a legitimate interest in using information relating to subject health and care for research studies, when subjects agree to take part in a research study. This means that we will use their data, collected in the course of a research study, in the ways needed to conduct and analyze the research study. Subject’s rights to access, change or move their information are limited, as we need to manage such information in specific ways in order for the research to be reliable and accurate. If a subject withdraws from the study, we will keep the information about them that we have already obtained. To safeguard subject’s rights, we will use the minimum personally identifiable information possible.

If subjects wish to raise a complaint regarding how Invicro has handled their personal information, they can contact our Data Protection Officer who will investigate the matter. If subjects are not satisfied with our response or believe we are processing personal information in a way that is not lawful they can complain to the National Data Protection Agency, e.g. Information Commissioner’s Office (ICO) in the United Kingdom.

Marketing

If you decide to provide us your contact details for direct marketing purposes, and consent for us to do so, we would like to keep in touch with you regarding the latest news and information from our organization. Minimal, non-sensitive information will be retained to fulfil the requirements of this legitimate interest, and data will not be shared with third parties without notification and appropriate consent of the data subject.

Recruitment

Your personal data may be processed in relation to job vacancies that you have applied for, generally processing any job applications, facilitating the recruitment process and furthering our relationship with you. The legal basis for this processing is our legitimate interests in finding an appropriate person for a particular role.

Where you have provided your consent for us to do so, we may consider you for opportunities that you did not specifically apply for but which we think might be a good fit for your skillset.

Where you have given us consent to process your information for the purposes detailed above, we will enter the profile data into our central recruitment database.

We may collect your details, that you have made available, from third-party sources such as websites on which our vacancies may be advertised, or through recruitment agencies. This information may include your name, email address, telephone number, and curriculum vitae. We may do this where we identify that you are suitable for an available vacancy with us. We may use the contact data to contact you to ask whether you would like to be considered for an appropriate vacancy. Our use of the contact data in these circumstances is limited to making contact with you to determine whether you are interested in working for us and applying for a role. The legal basis for this processing is our legitimate interest as a business in finding an appropriate person for a particular role.

Data Retention: We only retain personal data for as long as is necessary for us to render a service you have requested or to which you have given your consent, except where otherwise provided by law (e.g. in connection with pending litigation).

Notice

Invicro will inform individuals about:

- the right of individuals to access their personal information, as required by applicable regional regulations and laws.
- how Invicro will use information from subjects in order to undertake research. When Invicro is the sponsor of the study we will act as the data controller for this study. This means that Invicro is responsible for looking after subject information and using it properly.
- data retention including that Invicro may need to keep study data after the study has completed according to the relevant regulatory requirements.
- their rights to access, change or move their information, including that, for research data, such actions are limited, as Invicro needs to manage subject information in a specific way in order for research to be reliable and accurate.

- subject data obtained in the study, if the subject withdraws from the study. This would include Invicro maintaining the existing information about the subject obtained prior to the withdrawal.
- that Invicro will safeguard the subject's rights, including using the minimum personally identifiable information possible.
- the organization being subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC)
- the requirement for the organization to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements
- the organization's liability in cases of onward transfers to third parties
- the possibility, under certain conditions, for the individual to invoke binding arbitration for complaints regarding Privacy Shield compliance not resolved by any of the other Privacy Shield mechanisms. For additional information: https://www.privacyshield.gov/article?id=ANNEX-I-introduction
- the requirement for the organization to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements
- in the context of an onward transfer, the organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. As a Privacy Shield organization, Invicro shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.

Invicro will include a notice to individuals regarding the purposes for which we collect and use Personal Information about them, how to contact us, the types of third parties with whom we may share Personal Information (if applicable), and any ways that individuals may limit the use and sharing of such information. This notice will be provided when individuals are first asked to provide Personal Information or as soon thereafter as is practicable.

Consent/ Choice

Collection and retention of personal information at Invicro will be done so according to the relevant legal basis. Notice of the relevant legal basis will be available to individuals. If that legal basis is consent, individuals will receive an appropriate level of information about the use of their personal information and have their consent/choice to collect and retain the data documented. This consent may be

withdrawn at any time, and if the legal basis for retention of data is consent, this data will no longer be retained by Invicro.

Where consent is not the legal basis, Invicro may decide that documented consent is best practice, or in the case of research subjects, a regulatory requirement, and therefore consent would also be sought from individuals. It will be explained to subjects, in this instance, that although consent is sought, data may still be used and retained by Invicro if there is an additional legal basis for these activities.

Onward Transfer

Invicro will only transfer Personal Information to a third party consistent with the notice and consent principles stated above. If Invicro discloses Personal Information to a third party, Invicro will either: (i) ensure that the third party is subject to the privacy principles; or (ii) require the third party by contract to provide the same level of protection as required by the privacy principles.

Transfers Outside the European Economic Area

Where your personal data is transferred outside of the EEA, we will ensure that either (a) The European Commission has made an "adequacy decision" with respect to the data protection laws of the country to which it is transferred, or (b) we have entered into a suitable data processing agreement with the third party situated in that country to ensure the adequate protection of your data. This may include our Holding Company Invicro LLC based in the USA, whose data processing activities accord with the Privacy Shield. In all cases, transfers outside of the EEA will be protected by appropriate safeguards.

Please acknowledge that personal data that you submit for publication through our website or services may be publicly available, via the internet, around the World. We cannot prevent the use (or misuse) of such personal data by others.

Security

Invicro will take reasonable precautions to protect Personal Information from loss, misuse and unauthorized access, disclosure, alteration and destruction. The principle of security applies to how Invicro stores, processes, maintains and protects personal information.

Data Integrity

Invicro will only use and share Personal Information about individuals in a way that is consistent with the purposes for which the information was collected or subsequently authorized by those individuals. To the extent necessary for those purposes, Invicro will take reasonable steps to ensure that the information is accurate, complete, and current.

Access

Invicro will provide individuals with reasonable access to Personal Information as defined by any additional agreements (i.e. Informed Consent Form) about them and they may request the correction or amendment of Personal Information that they demonstrate to be incorrect or incomplete.

Enforcement

Invicro has put in place mechanisms to verify our ongoing adherence to these privacy principles. We encourage individuals covered by this statement to raise any concerns that they have about the way we process their Personal Information by contacting us at the address below, and we will do our best to resolve them. We have also agreed to participate in the independent dispute resolution program provided by the European Data Protection Authorities Panel, and the Swiss equivalent.

In compliance with the Privacy Shield Principles, the Invicro Entities commit to resolve complaints about your privacy and our collection or use of your Personal Information transferred to the United States pursuant to Privacy Shield. European Union and United Kingdom, and Swiss individuals with Privacy Shield inquiries or complaints should first contact us at [dpo@invicro.com].

Adherence by Invicro to these privacy principles may be limited to the extent required to meet a legal, governmental, national security or public interest obligation.

Collection of Online Data

You are not required to provide personal information as a condition of using our site, except as may be necessary to provide you a product or service at your request. When you use our website, data may be stored for various security purposes. This data may include the name of your internet service provider, the web site that you used to link to our site, the web sites that you visit from our site and your IP-Address. This data could possibly lead to your identification, but we do not use it to do so. We do use the data from time to time for statistical purposes but maintain the anonymity of each individual user. In cases when personal information is provided to others to provide you products or services you have requested, or for other purposes you have authorized, we rely on technical and organizational means to assure that applicable data security regulations are followed. Your IP address is utilized for security and performance measurement with a 4-week retention on this information.

Collection and Processing of Personal Information Online

We collect personal information only when you provide it to us, through registration, completion of forms or e-mails, as part of an order for products or services, inquiries or requests about materials being ordered and similar situations in which you have chosen to provide the information to us.

The database and its contents remain at our company and stay with data processors or servers acting on our behalf and responsible to us. Your personal information will not be passed on by us or by our agents

for use by third parties in any form whatsoever, unless we have obtained your consent or are legally required to do so.

We will retain control of and responsibility for the use of any personal information you disclose to us. Some of this data may be stored or processed at computers located in other jurisdictions, such as the United States, whose data protection laws may differ from the jurisdiction in which you live. In such cases, we will ensure that appropriate protections are in place to require the data processor in that country to maintain protections on the data that are equivalent to those that apply in the country in which you live.

Your Rights

You may instruct us to provide you with any personal information we hold about you; provision of such information will be subject to:

(a) your request not being found to be unfounded or excessive, in which case a charge may apply; and

(b) the supply of appropriate evidence of your identity (for this purpose, we will usually accept a photocopy of your passport certified by a solicitor or bank plus an original copy of a utility bill showing your current address).

We may withhold personal information that you request to the extent permitted by law, or where it might involve another individual's personal data

You may instruct us at any time not to process your personal information for marketing purposes.

In practice, you will usually either expressly agree in advance to our use of your personal information for marketing purposes, or we will provide you with an opportunity to opt out of the use of your personal information for marketing purposes.

The rights you have under data protection law are:

(a) the right to access;

(b) the right to rectification;

(c) the right to erasure;

(d) the right to restrict processing;

(e) the right to object to processing;

(f) the right to data portability;

(g) the right to complain to a supervisory authority; and

(h) the right to withdraw consent.

Your right to access your data. You have the right to ask us to confirm whether or not we process your personal data and to have access to the personal data and any additional information. That additional information includes the purposes for which we process your data, the categories of personal data we hold and the recipients of that personal data. You may request a copy of your personal data. The first copy will be provided free of charge, but we may charge a reasonable fee for additional copies.

Your right to rectification. If we hold any inaccurate personal data about you, you have the right to have these inaccuracies rectified. Where necessary for the purposes of the processing, you also have the right to have any incomplete personal data about you completed.

Your right to erasure. In certain circumstances you have the right to have personal data that we hold about you erased. This will be done without undue delay. These circumstances include the following: it is no longer necessary for us to hold those personal data in relation to the purposes for which they were originally collected or otherwise processed; you withdraw your consent to any processing which requires consent; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are certain general exclusions of the right to erasure, including where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for establishing, exercising or defending legal claims.

Your right to restrict processing. In certain circumstances you have the right for the processing of your personal data to be restricted. This is the case where: you do not think that the personal data we hold about you is accurate; your data is being processed unlawfully, but you do not want your data to be erased; it is no longer necessary for us to hold your personal data for the purposes of our processing, but you still require that personal data in relation to a legal claim; and you have objected to processing, and are waiting for that objection to be verified. Where processing has been restricted for one of these reasons, we may continue to store your personal data. However, we will only process it for other reasons: with your consent; in relation to a legal claim; for the protection of the rights of another natural or legal person; or for reasons of important public interest.

Your right to object to processing. You can object to us processing your personal data on grounds relating to your particular situation, but only as far as our legal basis for the processing that it is necessary for: the performance of a task carried out in the public interest, or in the exercise of any official authority vested in us; or the purposes of our legitimate interests or those of a third party. If you make an objection, we will stop processing your personal information unless we are able to demonstrate compelling legitimate grounds for the processing, and that these legitimate grounds override your interests, rights and freedoms; or the processing is in relation to a legal claim.

Your right to object to direct marketing. You can object to us processing your personal data for direct marketing purposes. If you make an objection, we will stop processing your personal data for this purpose.

Your right to object for statistical purposes. You can object to us processing your personal data for statistical purposes on grounds relating to your particular situation, unless the processing is necessary for performing a task carried out for reasons of public interest.

Effective: July 2020
Last Updated: 30 July 2020

Automated data processing. To the extent that the legal basis we are relying on for processing your personal data is consent, and where the processing is automated, you are entitled to receive your personal data from us in a structured, commonly used and machine-readable format. However, you may not have this right if it would adversely affect the rights and freedoms of others.

Complaining to a supervisory authority. If you think that our processing of your personal data infringes data protection laws, you can lodge a complaint with a supervisory authority responsible for data protection. You may do this in the EU member state of your habitual residence, your place of work or the place of the alleged infringement.

Right to withdraw consent. To the extent that the legal basis we are relying on for processing your personal data is consent, you are entitled to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

Exercising your rights. You may exercise any of your rights in relation to your personal data by written notice to us in addition to the other methods specified above.

Google Analytics

Invicro uses Google Analytics to analyze user activity in order to improve our website. For example, using cookies we can look at aggregate patterns and page performance trends. We can use such analysis to gain insights about how to improve the functionality and experience of the website. No personal information is taken from visitors from a website utilizing Google Analytics, nor is it stored. For information on how to opt-out of Google Analytics tracking, please visit this link - https://www.invicro.com/privacy-policy#GA"

Use of Cookies

Cookies are small text files that are stored in the visitor's local browser cache. Using such cookies, it is possible to recognize the visitor's browser in order to optimize the website and simplify its use. Data collected via cookies will not be used to determine the personal identity of the website visitor.

Most browsers are set-up to accept these Cookies automatically. In addition, you can deactivate the storing of cookies or adjust your browser to inform you before the Cookie is stored on your computer.

Children's Online Privacy Protection

In light of the importance of protecting children's privacy, we do not collect, process or use on our website any information relating to an individual whom we know to be under 13 years old without the prior, verifiable consent of his or her legal representative. Such legal representative has the right, upon request, to view the information provided by the child and/or to require that it be deleted.

Effective: July 2020
Last Updated: 30 July 2020

How to Contact Us

Initial questions, comments or complaints regarding collection and processing of your information should be directed to:

Data Protection Officer:

Matt Chernesky, Senior Director of Information Technology
Invicro
60 Temple Street
Suite 8B
New Haven, CT 06510

Email: dpo@invicro.com
Telephone: 203-508-1520
Fax: 203-789-8037

Roughan Sheedy, Chief Commercial Officer
Invicro
27 Drydock Avenue
Boston, MA 02210

Email: dpo@invicro.com
Telephone: 617-777-2783

Changes to this Statement

This Statement may be amended from time to time, consistent with the requirements of the Privacy Shield. When we do, we will also revise the "last updated" date at the bottom of this Statement. For material changes to this Statement, we will notify individuals by placing a notice on this page.

Effective: July 2020
Last Updated: 30 July 2020