Diligent Third Party Risk Intel – Privacy Policy Supplement

1. Scope

This Privacy Policy Supplement applies solely to Third Party Risk Intel – Individual Screening provided by Diligent Group Companies that screens natural persons (individuals) against sanctions lists, watchlists, or adverse media for our clients' due diligence or compliance purposes. (the "Individual Screening Product").

For the avoidance of doubt, this Policy does not apply to (i) Diligent's entity-level or company risk assessment tools, whose primary function is to assess, score, or report on legal entities, organisations, or companies rather than natural persons, (ii) any compliance related databases provided by Diligent Group Companies such as info4c Products, and (iii) any Diligent product or service where Diligent processes personal data solely in the capacity of a data processor acting on client (data controller) instructions, such as Diligent Compliance Products, including Diligent Due Diligence and Third Party Manager.

2. Diligent's Role as Data Controller

Diligent acts as an independent data controller for the processing activities carried out in connection with the Individual Screening Product.

Diligent's customers use the Individual Screening Product to fulfil their own regulatory and compliance obligations (these include, but are not limited to anti-money-laundering, financial crime, terrorist financing, anti-corruption, anti-fraud, know-your-customer, or sanctions legislation). The Individual Screening Product assists and are necessary to enable and assist our clients in meeting these obligations.

Where a client submits identifying information about a screening subject (e.g. name, nationality, contextual information) to initiate a screening, Diligent also acts as a data processor in respect of that submitted personal data, processing it on the customer's instructions. Our client is the data controller for processing activities carried out on such data.

3. Who we process information about

The Individual Screening Product processes information about individuals identified by our clients as a screening subject indicating that information relating to such individuals is relevant to our clients' compliance or due diligence checks.

This typically includes individuals who may fall into one or more of the following categories:

- Politically Exposed Persons (PEPs): individuals who hold or have held prominent public functions as defined under applicable legislation. Close family members and known close associates may also be included where required by law.
- Sanctioned individuals: persons named on official government or international sanctions lists, including those issued by the UN, EU, UK (OFSI), and US (OFAC).
- Watchlist subjects: individuals appearing on watchlists maintained by regulators, law enforcement agencies, or government bodies in connection with money laundering, terrorist financing, bribery, corruption, fraud, or financial crime.
- Adverse media subjects: individuals about whom credible authoritative public sources report actual or alleged involvement in financial crime, serious fraud, bribery, corruption, or related misconduct.

Inclusion in screening results does not automatically prevent you from doing business with our clients such as financial institutions. Diligent's clients are responsible for conducting their own independent assessments using screening outputs as one input among many. Our clients make their own decisions about how to use the data they receive from us in order to conduct their compliance and due diligence checks. If you have any questions about these decisions, please refer them to the relevant Diligent client.

4. Personal data we process

Individual Screening Product may process the following additional categories of personal data:

- Identifying and professional data: your name, your nationality, date of birth, country of your location, current organization and position, professional experience, professional specialization, other information that our clients provide us at their option when conducting a screening.
- Sanctions, watchlist and blacklist data:
    - (i) sanctions data is about inclusion on any official sanctions lists, watchlists, debarment registers, or lists of disqualified persons. It is data that we collect about you as being subject to financial sanctions according to major financial sanctions lists, such as full name, other names, ID, type of SDN or entity, address, name of the financial sanction list in which it appears, type of list, date of publication, authority. We collect sanction data from regulators and other official national and international organizations and institutions.

(ii) Watchlist and blacklist data is data we collect about you in relation to warning notices from financial authorities and supervisors (e.g. Bafin, FMA, CBFEA, FINMA, CNMV, MAS, FCA), wanted lists from police departments, governments, national and international investigation authorities (e.g. Interpol, FBI, DEA, DIA), as well as lists from international tribunals, enforcement actions, disqualified directors from governmental and international agencies, such as first name, last name, other names, date of birth, country, category, title, ID, alternative script, description of the case, name of the list, date of information and authority. We collect watchlist and blacklist data from official, recognized and documented sources.

- Adverse media data: information, sourced from publicly available news articles, about alleged or actual criminal activities, regulatory breaches, fraud, corruption, other behaviours that may present financial or reputational risks.
- PEP specific information: whether you are/were a PEP or are a close relation or associate of a PEP, marital status or other details of PEP relations, associates and dependants, and PEP relevant commercial information, such as: (i) ownership or control of companies, partnerships, or trusts, (ii) directorships or executive roles, (iii) business ventures in which the individual holds a financial interest, (iv) associations with sanctioned entities.
- Inferred information on political opinions (e.g. where an individual holds or has held a prominent political role).
- Inferred information on religious or philosophical beliefs (e.g- where a senior religious figure qualifies as a PEP).
- Trade union membership (where a senior trade unionist qualifies as a PEP under applicable laws).
- Information relating to actual criminal offences or alleged offences derived from official court, regulatory, or law enforcement records.

In some cases, the personal information we collect constitutes, depending on specific jurisdictions and their applicable data protection laws, special categories of personal data (for example your political opinions), meaning information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic or biometric data for the purpose of uniquely identifying a natural person, or data concerning health or sex life or sexual orientation. Such special category personal data sourced from publicly available sources (such as official government, regulatory and court records, and whitelisted news sources). This may include information about political opinions (for example, where an individual holds or has held a prominent political role). Processing of such data is carried out on the basis that it is necessary for reasons of substantial public interest under applicable law.

In certain circumstances, we may also process information relating to any criminal offences actually or allegedly committed by you.

5. Legal basis for processing

Standard personal data

Diligent processes standard personal data as an independent controller on the basis of legitimate interests. These relevant legitimate interests are:

- The interests of Diligent's customers in fulfilling their legal and regulatory compliance obligations (including AML, KYC, sanctions, and ABAC obligations imposed by applicable law).
- The broader public interest in preventing and detecting financial crime, money laundering, bribery, corruption, fraud, and sanctions evasion.
- Diligent's own commercial interest in providing risk intelligence and due diligence tools that support those compliance objectives.

Special category data

Where processing involves special category personal data, Diligent relies on the substantial public interest where processing is necessary for compliance with regulatory obligations relating to the prevention or detection of financial crime, money laundering, bribery, corruption, or sanctions evasion.

Criminal offence data

Processing of data relating to criminal offences or allegations is carried out only to the extent authorised under applicable law (including national anti-money-laundering and compliance legislation).

6. Automated Decision Making

Diligent does not make solely automated decisions that produce legal or similarly significant adverse effects on you. The Individual Screening Product generates summaries and structured outputs as analytical aids; they do not make detrimental recommendations or decisions concerning you.

Notwithstanding the above, Diligent provides the following transparency information about the automated components of the Individual Screening Product:

- The credibility relevance score in some Individual Screening Product is determined by automated term-matching logic, not by human editorial judgment.
- The AI-generated summary is produced by a large language model and reflects the system's synthesis of sourced content; it should be treated as an analytical starting point, not a verified conclusion.
- To the extent available in the Individual Screening Product, the identity disambiguation step (matching candidate profiles based on user-provided identifiers) involves automated candidate generation followed by mandatory user selection of the correct individual.

7. Profiling

The Individual Screening Product may involve profiling within the meaning of applicable EU legislation — that is, automated processing of personal data to evaluate certain personal characteristics relating to the individual. Specifically, the products evaluate characteristics relating to an individual's professional conduct, public role, regulatory status, and potential involvement in financial crime or serious misconduct, for the purpose of assessing compliance and due diligence risk. The output of this profiling is intended solely as an analytical aid for the customer's human reviewers.

The legal basis for profiling is legitimate interests (as described in Section 4 above). You have the right to object to profiling on the basis of you particular situation under some local, data protection legislation (including the EU and UK), subject to the balancing exercise described in Section 9 below.

8. How we use your personal data

We mainly use your personal information to facilitate screenings run by our clients which includes the following activities:

- Performing sanctions, watchlist, and adverse media checks at the request of our clients.
- Generating structured screening reports for our clients' review.
- Responding to data subject enquiries and correction requests.

- Complying with requests from courts, regulators, law enforcement, and other public bodies or complying with fraud prevention checks or comply with other legal or regulatory requirements.
- We may use your personal information to exercise our legal rights where it is necessary to do so, for example to detect, prevent and respond to fraud claims, intellectual property infringement claims or violations of law or our applicable contract terms and conditions.
- Other activities necessary for the improvement of our service, including service testing, analytics and use of artificial intelligence and machine learning capabilities. It is in our legitimate interest to use the information provided to us for this purpose, so we can provide an improved experience for our customers and understand any issues with our services and improve them.

Personal data is deleted at the end of the relevant client subscription in relation to which the screening was conducted or earlier if applicable law, our retention schedule or our client requires so.

9. Your Rights

If your personal data is processed in connection with the Individual Screening Product, you have the rights set forth below in accordance with applicable data protection law. Subject to local law, these rights may include the right to:

- access your personal data;
- rectify the information we hold about you;
- erase your personal data;
- restrict our use of your personal data, including limiting disclosures made for valuable consideration;
- object to our use of your personal data;
- receive your personal data in a usable electronic format and transmit it to a third party (right to data portability);
- object to profiling (we shall no longer process the personal data unless we demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or as needed for the establishment, exercise or defence of our legal claims).
- receive a disclosure regarding how we have collected and used your personal data; and/or
- lodge a complaint with your local data protection authority.

When you contact us to exercise these rights, we will request information to verify your identity before processing your request. Once we verify your request, we will comply with it to the extent required by applicable law. In some cases, we may be prohibited from disclosing certain information, or may be permitted to retain information, for example to complete the processing for which it was provided or to comply with a legal obligation.

If you are a California resident, we will not deny you goods or services, charge a different price or rate, or provide a different level or quality of goods or services on account of your decision to exercise any of the rights that may apply to you.

To exercise any of these rights, contact us at the contacts specified under Section 10 of the Policy above.

10. Information We Disclose

We may disclose your personal data to the following categories of recipients:

- Diligent group companies, for the provision of the Individual Screening Product, customer support, internal reporting and insights, and service optimisation. A list of companies within the Diligent group can be found at https://www.diligent.com/diligent-data-controllers.
- The Diligent customer that has requested the screening to which your personal data relates.
- We disclose your personal information with our vendors and service providers who provide products and services that we use to operate our business and carry out the purposes listed above.
- Law enforcement agencies, courts, regulators, government authorities or other third parties, where we believe this is necessary to comply with a legal or regulatory obligation, or otherwise to protect our rights or the rights of any third party. Where permitted by law and reasonably practicable, we will attempt to notify you of such requirements.
- Asset purchasers, being any third party that purchases, or to which we transfer, all or substantially all of our assets and business. Should such a sale or transfer occur, we will use reasonable efforts to ensure that the recipient uses your personal data in a manner consistent with this Policy.

Because we operate as part of a global business, the recipients referred to above may be located outside the jurisdiction in which you are located. See the section on International Data Transfers below for more information.

11. Information Security and Retention

We implement technical and organisational measures to ensure a level of security appropriate to the risk to the personal data we process. These measures are aimed at ensuring the ongoing integrity and confidentiality of personal data, and we evaluate them on a regular basis to ensure the security of the processing.

We retain personal data processed in connection with the Individual Screening Product for as long as necessary for the purposes for which it was collected, taking into account the amount, nature and sensitivity of the relevant personal data. Where we collect personal data from third-party or publicly available sources and do not have a relationship with you, we will keep it for a period of time that is consistent with the reason for which we collected it. When these retention periods have ended, we may retain your personal data for a further period of time that enables us to:

- maintain business records for analysis and/or audit purposes;
- comply with record-retention requirements under the law;
- defend or bring any existing or potential legal claims;
- deal with any complaints regarding the Individual Screening Product; and
- enforce our commercial agreements.

We will delete your personal data when it is no longer required for these purposes. If there is any information that we are unable, for technical reasons, to delete entirely from our systems, we will put in place appropriate measures to prevent any further processing or use of the data.

12. International Data Transfers

Your personal data may be transferred to, stored and processed in various countries, including those that are not regarded as ensuring an adequate level of protection for personal data under European Union or United Kingdom law. We have put in place appropriate safeguards (such as the European Commission's Standard Contractual Clauses and other contractual commitments) in accordance with applicable legal requirements to ensure that your personal data is adequately protected. For more information on the appropriate safeguards in place, please contact us using the details below.

13. EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. Data Privacy Framework

Diligent Corporation ("Diligent") complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Diligent has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. DPF Principles with regard to the processing of personal data received from the European Union and the United Kingdom, and to the Swiss-U.S. DPF Principles with regard to personal data received from Switzerland. If there is any conflict between the terms in this Policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework programme and to view our certification, please visit https://www.dataprivacyframework.gov/.

In the context of an onward transfer, Diligent is responsible for the processing of personal data it receives under each Data Privacy Framework and subsequently transfers to a third party acting as an agent on its behalf. Diligent remains liable under each respective Data Privacy Framework if its agent processes personal data in a manner inconsistent with that Framework, unless Diligent proves that it is not responsible for the matter giving rise to the damage.

With respect to personal data received or transferred under the Data Privacy Frameworks, Diligent is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, Diligent may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with the Data Privacy Frameworks, Diligent commits to cooperate and comply with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC), as applicable, with regard to unresolved complaints. Under certain conditions, you may be entitled to invoke binding arbitration when other dispute-resolution procedures have been exhausted. As of the date of this Policy, Diligent does not rely on the Swiss-U.S. DPF as a data-transfer mechanism in accordance with the laws of Switzerland.

14. Contact Us

Diligent Corporation and, with respect to service-specific inquiries or relationships, the relevant group companies available at https://www.diligent.com/diligent-data-controllers, are the controllers responsible for the personal data processed in connection with the Individual Screening Product.

Our European Union representative is Diligent Governance Ireland Limited, whose registered office is located at 6th Floor, South Bank House, Barrow Street, Dublin 4, Ireland.

Our United Kingdom representative is Diligent Boardbooks Limited, whose registered office is located at 25 Bedford Street, London, England WC2E 9ES, United Kingdom.

Our Data Protection Officer can be contacted at privacy@diligent.com.

If you have questions or concerns regarding the way in which your personal data has been used, or if you wish to exercise any of your rights, please submit your request at https://www.diligent.com/contact-legal. Alternatively, you may reach us through our support phone number (1.866.262.7326). We will take steps to verify your identity before addressing your request. We are committed to working with you to obtain a fair resolution of any complaint or concern about privacy; if you believe we have not been able to assist, you have the right to make a complaint to your local data protection authority.

15. Changes to this Policy

You may request a copy of this Policy from us using the contact details set out above. We may modify or update this Policy from time to time.