Holland & Knight LLP

Personnel Data Protection Policy

1. DATA PROTECTION PRINCIPLES

Holland & Knight LLP (the "Firm") requires that any client using an e-billing system, and each e-billing Vendor client selects for working with the Firm, adheres to the following principles when processing the personal data of Holland & Knight personnel:

1.1 Lawfulness, fairness and transparency – data must be processed lawfully, fairly and in a transparent manner.

1.2 Purpose limitation - data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

1.3 Data minimization - data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

1.4 Accuracy - data must be accurate and, where necessary, kept up to date.

1.5 Storage limitation - data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information are processed.

1.6 Integrity and confidentiality - data must be processed in a manner that ensures appropriate security of the personal information, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage by using appropriate technical or organizational measures.

2. INFORMATION COLLECTED

2.1 A client and its e-billing vendor may collect personal information of Firm personnel to manage and operate the client's business.

2.2 The personal information of Firm personnel that is collected in the course of the Firm's representation of client may include, but is not limited to, the following:

- name;
- business address;
- contact details (such as telephone numbers and email address);
- personally identifiable information including gender, date of birth, race/ethnicity, citizenship, sexual orientation and gender identity, disability status, and military service;
- other personal information contained in correspondence and documents which the Firm may provide to the client; and
- information obtained from the client's IT and communications monitoring.

2.3 This personal information is required by the client to allow the Firm to provide our service to the client. If the Firm does not provide personal information as requested by the client, it may delay payment of the Firm's invoices by the client.

3. HOW INFORMATION IS COLLECTED

The client and its e-billing vendor collects most of this information from through the e-billing system, however, information may also be collected:

3.1 From information the Firm provides to the client (via email, correspondence, or other forms of communication) in response to specific inquiries by the client;

3.2 from publicly accessible sources;

3.3 directly from a third party, e.g. vendor due diligence providers;

3.4 via the Firm's website (e.g., through the use cookies);

3.5 via information technology systems, e.g.:

- online case management, document management and time recording systems;
- door entry systems and reception logs; and
- CCTV and access control systems.

4. SPECIAL CATEGORIES OF ("SENSITIVE") PERSONAL INFORMATION

The Firm may also supply the client and its e-billing vendor with, or they may receive, special categories of "sensitive" personal information. These special categories of personal information may be provided on the basis of one or more of the following:

4.1 where Firm personnel have given explicit consent to the processing of the personal information for one or more specified purposes;

4.2 where the processing relates to personal information which is manifestly made public by Firm personel;

4.3 where the processing is necessary for the establishment, exercise or defence of legal claims; or

4.4 where the processing is necessary for reasons of substantial public interest, in accordance with applicable law. Such reasons include where the processing is necessary:

- for the purposes of the prevention or detection of an unlawful act or for preventing fraud; and
- for the provision of confidential advice.

5. DATA RELATING TO CRIMINAL CONVICTIONS & OFFENCES

Client and its e-billing vendor may collect and store personal information relating to criminal convictions and offences (including the alleged commission of offences) only where necessary for the purposes of:

5.1 the prevention or detection of an unlawful act and as necessary for reasons of substantial public interest;

5.2 providing or obtaining legal advice; or

5.3 establishing, exercising or defending legal rights.

6. HOW AND WHY PERSONAL INFORMATION MAY BE USED

6.1 Client and its e-billing vendor's use of the personal information of Firm personnel is subject to the Firm's instructions, data protection laws and the duties of confidentiality provided for in this Policy.

6.2 Client and its e-billing vendor will only process the personal information of Firm personnel if there is a legal basis for doing so, including where:

- processing is necessary for the performance of the Firm's contractual engagement with the client;

- processing is necessary for compliance with a legal obligation to which the client is subject; or

- processing is necessary for the purposes of the legitimate interests pursued by the client except where such interests are overridden by the interests of the Firm's personnel or fundamental rights and freedoms.

6.3 Where client requests personal information of Firm personnel for compliance with anti-money laundering regulations, client shall process such information only for the purposes of preventing money laundering or terrorist financing, or as otherwise set out in this Policy or permitted by law.

7. THIRD PARTY PROCESSORS

Where processing of personal information of Firm personnel is carried out by a third party data processor on behalf of client or its e-billing vendor, client will endeavour to ensure that appropriate security measures are in place to prevent unauthorized access to or use of the data.

8. DISCLOSURE OF PERSONAL INFORMATION

8.1 Personal information of Firm personnel will be retained by client and its e-billing vendor and will not be shared, transferred or otherwise disclosed to any third party, except as set out in this Policy.

8.2 Client and its e-billing vendor may disclose and share personal information of Firm personnel, if acting in good faith, consider disclosure to be required by law or the rules of any applicable governmental, regulatory or professional body.

8.3 Should client or its e-billing vendor be requested by certain authorities to provide them with access to personnel information of Firm personnel in connection with the work the Firm has done for client, or are doing, for client, client and its e-billing vendor will comply with that request only to the extent that it is bound by law to do so and, in so far as it is allowed, will notify the Firm of that request or provision of information.

8.4 Client and its e-billing vendor will only allow its service providers to handle personal information of Firm personnel if satisfied that they take appropriate measures to protect the personal information of Firm personnel. Client and its e-billing vendors also impose contractual obligations on service providers to ensure they can only use the personal information of Firm personnel to provide services to the client, it's e-billing vendor and the Firm.

8.5 Client or its e-billing vendor may also need to share some personal information of Firm personnel with other parties, such as potential buyers of some or all of client's or its e-billing vendor's business or during a re-structuring. The recipient of the information will be bound by confidentiality obligations.

9. SECURITY OF INFORMATION

9.1 Client and its e-billing vendor may store personal information of Firm personnel in physical and digital formats. Information may be held at the offices of client and it's e-billing vendor in the United States. Client and its e-billing vendor use industry standard technical and organizational measures to protect information from the point of collection to the point of destruction. For example:

- appropriate, encryption, firewalls, access controls, policies and other procedures to protect information from unauthorized access.

- where appropriate, pseudonymisation and / or encryption to protect the information.

9.2 Client and its e-billing vendor will only transfer personal information to a third party if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

10. INFORMATION RETENTION PERIODS

10.1 Personal information of Firm personnel received by client and it's e-billing vendor will only be retained for as long as necessary to the Firm's representation of client. Following the end of the Firm's representation of client, client and its e-billing vendor will retain the personal information of Firm personnel:

- to enable us to respond to any queries, complaints or claims made by or on behalf of the Firm or Firm personnel; and
- to the extent permitted for legal, regulatory, fraud and other financial crime prevention and legitimate business purposes.

10.2 After this period, when it is no longer necessary to retain the personal information of Firm personnel, client and its e-billing vendor will securely delete or anonymise it in accordance with their data retention policies.