# Holland & Knight Data Protection Policy

Updated as of January 1, 2023

## Policy Statement

The Holland & Knight Data Protection Policy (the "Policy") is intended to help everyone protect personal information and should be used as a guide in our daily practices. This Policy explains your obligations to safeguard and protect personal information.

## Scope

This Policy applies to everyone that handles personal information on behalf of Holland & Knight LLP and our associated affiliates[1] (the "Firm") in support of business operations or the provision of professional services by the Firm to our clients. This Policy applies to Firm personnel, clients and the service providers used by clients, including e-billing providers.

## Duty to Safeguard and Protect Confidential Information

Much of the data and information received, created, used, transmitted and maintained with respect to the Firm and Firm Personnel is confidential. Almost all data associated with a client representation is considered confidential in nature. The rules of professional conduct impose a duty on lawyers and law firms to preserve and protect client confidential information. All non-public, confidential Firm information and confidential client information ("Confidential Information") must be protected, and treated as confidential. You should endeavor to safeguard and not disclose or permit unauthorized access to Confidential Information.

## Definition of Personal Information

Additionally, personal information with respect to individuals should be accorded an even greater standard of care than that applied to other Confidential Information.

Personal information may be specifically defined under various laws, but for purpose of this Policy, the defined term **"Personal Information"** or **"PI"** is a fact about an individual, which if combined with one or more other facts about that individual, would enable others to determine the specific person to whom the facts apply. Examples of Personal Information include the following (all of which are collectively included within the defined term Personal Information):

a. Commonly available and the least sensitive forms of Personal Information, routinely used in the daily activities of Firm Personnel on behalf of the Firm and Firm clients (referred to herein as "**Common Personal Information"**) such as Name, Address, Phone Number, Email Address, and IP Address[2];
b. **"Sensitive Personal Information"** or **"SPI"** such as:

[1] Including Holland & Knight (UK) LLP, Holland & Knight Colombia S.A.S. and Holland & Knight Mexico S.C.

[2] Common Personal Information is widely available from numerous sources other than the Firm and it is pervasive in the routine operations of the Firm. While Common Personal Information is included within the definition of Personal Information, the Firm has determined that, in most cases, the characteristics of Common Personal Information mitigate in favor of it being subject to the duties and restrictions applicable to Confidential Information rather than those applicable to other Personal Information.

- Date of Birth and Marital Status;
- Social Security Numbers or Tax Code;
- Driver License, State-Issued Identification Number or Passport Data;
- Financial Accounts, Debit and Credit Card Numbers;
- Information about an individual's health condition, medical treatment options, or course of medical treatment (referred to herein as "**Health Information**").

c. Health Information governed by the Health Information Portability and Accountability Act (HIPAA), referred to herein as **"Personal Health Information"** or **"PHI"**; and

d. Special Categories of Personal Information (requiring an even greater standard of care in handling, referred to herein as "**Special Category Information**" or **"SCI"**) such as Race or Ethnic Origin, Political Opinions, Religious of Philosophical Beliefs, Trade Union Membership, Genetic Data, Biometric Data, Data Concerning Sex Life, Gender Identification, Sexual Orientation, Veteran Status or Disability Status.

# Procedures

## 1. Privacy and Data Protection Principles

The Firm adheres to, and expects our clients and service providers to clients that process PI to comply with, industry-standard privacy data protection principles, including the following:

- Accountability**:** PI is collected and processed with appropriate controls and measures to demonstrate compliance with our legal and regulatory obligations.

- Accuracy and Quality**:** Subject to applicable privacy law, individuals have the right to access their PI to ensure its accuracy and completeness. When necessary, reasonable efforts are taken to ensure that inaccurate data is rectified in a timely manner.

- Data Minimization**:** PI is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

- Integrity and Confidentiality**:** PI is processed in a manner designed to provide appropriate security including protection against unauthorized or unlawful processing or access, accidental loss, destruction or damage, using appropriate technical and organizational measures.

- Lawfulness, Fairness and Transparency**:** PI is processed lawfully and fairly, with a valid legal basis and consent (where required), and information is provided about PI collection, use and disclosure through transparent notices. Individuals are given notice of privacy practices prior to any collection of PI to ensure privacy rights are clearly defined and individuals can make informed decisions about their PI. Opt-in and opt-out choices are provided to individuals with respect to their privacy rights under applicable privacy laws.

- Purpose Limitation and Specification**:** PI is collected for a specified, explicit and legitimate business purpose and there is a valid legal basis for the processing activity.

- Retention and Storage Limitation**:** PI is only retained for as long as necessary for the purposes it was collected, retention periods are applied and PI is securely destroyed once the retention period is satisfied.

## 2. Duty to Prevent Inadvertent Disclosure or Unauthorized Access

You should make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to PI including both digital and physical data. Inadvertent disclosure includes threats such as:

- Leaving a laptop or smartphone in a taxi or restaurant;
- Sending a confidential e-mail to the wrong recipient;
- Producing privileged documents or data in litigation; and
- Exposing confidential metadata.

Particular attention should be paid to avoiding inadvertent disclosure and unauthorized access of PI by adopting practices such as:

- Double checking email recipients before pressing send;
- When using email, viewing the full e-mail thread before forwarding, to ensure there is no information included that you would not intend to send to all recipients; and
- Reviewing all attachments and exhibits to documents and court filings to identify any unnecessary PI that has been included and should be redacted, anonymized or aggregated before sharing with others.

Firm policy restricts the use by Firm personnel of personal accounts such as personal webmail or cloud file-sharing platforms for the storage or transmission of any Confidential Information with respect to the Firm and Firm clients. PI should not be sent by Firm personnel to any personal account, nor saved to any personal devices (unless enrolled in the Firm's mobile device management program).

If you become aware of any inadvertent disclosure or unauthorized access, report it immediately to privacy@hklaw.com.

## 3. Duty to Safeguard and Protect Personal Information and Sensitive Personal Information

The Firm is subject to and complies with various privacy data protection laws worldwide. Please review the Holland & Knight Privacy Notice or visit Privacy at Holland & Knight for more information about our privacy practices.

You may come into contact with PI and SPI with respect to Firm personnel, vendors, clients, client customers, opposing parties, and representatives or other related parties of vendors, clients and opposing parties. You should ensure that:

- PI is processed only for the following purposes:
  - For the provision of professional services by the Firm to our clients;
  - For the administrative operations of a law firm in furtherance of providing professional services by the Firm to our clients;
  - At our instruction as the data controller; or
  - To satisfy a legal, regulatory or contractual obligation.

Access to Sensitive Personal Information, in digital or physical format, should be limited to only those with a reasonable "need-to-know" under the circumstances for efficient administration of the Firm, to accomplish the purpose for which the PI was collected or

received. Such access should be limited to only that which is necessary for the time period necessary. Consideration should be given to whether enhanced security protections should be utilized given the nature of the data. Enhanced security protections include (but are not limited to):

- Using encryption for electronic transmission;
- Securing digital documents with passwords;
- Applying restricted access rights to digital documents and databases using the principles of least-privileged access;
- Using pseudonyms instead of proper nouns;
- Redaction, anonymization and aggregation of PI, when applicable;
- Using data minimization techniques to collect, retain and use the minimum PI necessary; and
- Keeping physical documents in locked file cabinets at all times except when in active use.

Firm personnel should cultivate within your working groups an awareness of the importance of participating in Firm training and education about data security and privacy, and adopting a "Privacy by Design" mindset taking into consideration our duty to minimize and protect PI in our daily work by incorporating routine practices that support these considerations. If you have any questions about our privacy practices, or if you need guidance in meeting our legal, regulatory or client obligations, please contact privacy@hklaw.com for assistance.

## 4. Duty to Safeguard Protected Health Information

Protected Health Information contained in digital and physical data should only be received, used, stored and transmitted with appropriate protections and safeguards in place. The receipt, use, storage and transmission of PHI is governed by the Firm's Health Information Portability and Accountability Act (HIPAA) policies and procedures, and subject to the terms of the Business Associate Agreement (BAA) entered into between the Covered Entity and the Firm (or Business Associate of the Covered Entity and the Firm, as the case may be).

Access to PHI should only be granted on the basis of a reasonable "need-to-know" under the circumstances for efficient administration of the Firm. PHI may be used only for the purposes for which it was collected and consented to, and protected from unauthorized access or disclosure.

Additional safeguards may include:

- Data security (such as encryption) for data in transit and at rest;
- Using secure file-sharing solutions to transmit PHI;
- Data protection controls that limit the sharing or export of PHI; and
- Redaction, anonymization and other similar practices designed to promote 'Privacy by Design' principles, when applicable.

If you believe you may receive any PHI, contact privacy@hklaw.com for assistance.

## 5. Duty to Safeguard and Protect Special Category Information

For the purposes of data protection laws in the United Kingdom (UK) and Europe (EU), certain PI is treated as a Special Category Information to which additional protections apply under UK and EU data protection law.

Special Category Information includes:

- PI revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
- Genetic data and biometric data (when used to uniquely identify an individual); and
- Information concerning health, sex life or sexual orientation.

Access to SCI should be strictly limited to only those with an absolute "need-to-know". SCI must only be used for the purposes for which it was collected and consented to, and must be protected from unauthorized access and disclosure.

Additional safeguards should be used when handling SCI including encryption, access controls, secure transmission and storage, redaction, anonymization and other similar practices designed to promote data minimization and "Privacy by Design' principles.

If you believe you may receive any SCI, contact privacy@hklaw.com for assistance.

## 6. Disclosure of Personal Information of Firm Personnel

The Personal Information of Firm personnel is collected and retained by the Firm as a part of its business operations in support of the provision of professional services by the Firm to our clients (including SPI, PHI and SCI). If you have access to PI of Firm personnel, this PI may not be shared, transferred or otherwise disclosed to any other party, except as set out in this Policy, and your duties with respect to SPI, PHI and SCI of Firm Personnel are as provided herein.

In the context of the duties of Firm personnel on behalf of the Firm, you may have access to PI of Firm personnel. Firm personnel may disclose and share Common Personal Information of Firm personnel if acting in good faith and consider disclosure to be required by the duties of your position. Firm Personnel may share SPI, PHI and SCI of Firm personnel if acting in good faith and consider disclosure to be required by the duties of your position, and in accordance with procedures established within your work group, in accordance with this Policy and as approved by the Firm's General Counsel. Please contact privacy@hklaw.com for assistance.

As a client or a service provider to a client, you may be provided access to PI of Firm personnel. By receiving access to PI of Firm personnel, you are agreeing to act in good faith in using the PI of Firm personnel solely in support of the Firm's relationship with the client in providing professional services to the client, and in compliance with the duties with respect to SPI, PHI and SCI of Firm Personnel as provided herein. Such access should be limited to only that which is necessary for the time period necessary. At such time as you no longer have a good faith reason to retain PI of Firm personnel in support of the Firm's relationship with the client in providing professional services to the client, you will promptly and completely destroy all copies of such PI in a secure manner.

Clients and service providers of clients may disclose and share PI of Firm personnel, if acting in good faith and consider disclosure to be required by law or the rules of any applicable governmental, regulatory or professional body. Should you be requested by legal authorities to provide them with access to PI of Firm personnel in connection with the work the Firm has done or is doing for a client, client and its service providers may 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.

In the context of a sale or restructuring of a client or service provider to a client, any PI of Firm personnel shared with third parties remains subject to this Policy.

## 7. Service Providers

Where processing of PI is carried out by a third party service provider or data processor on behalf of the Firm or a client, appropriate technical, organizational, contractual and security measures should be in place to prevent unauthorized access to, disclosure of or use of PI.

Firm personnel with responsibility for contracting with third parties on behalf of the Firm or a client are required to confirm with the General Counsel that the third party takes appropriate measures to protect PI, and the Firm imposes contractual obligations to ensure they can only use our Firm or client PI to provide services to the client or the Firm. Please contact privacy@hklaw.com for assistance.

Clients may allow only your service providers to handle PI if you have made a good faith determination that they take appropriate measures to protect PI in accordance with this Policy, and if you impose contractual obligations on service providers to ensure they can only use our Firm or client PI to provide services to the client or the Firm.

## 8. Security and Incident Handling

Firm personnel shall immediately notify privacy@hklaw.com upon becoming aware of a potential incident involving the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, PI transmitted, stored or otherwise processed.

Clients and service providers to clients shall notify the Firm, without undue delay and within 72 hours, upon becoming aware of a confirmed incident involving the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, PI transmitted, stored or otherwise processed. You shall, at your own expense, provide the Firm with (i) sufficient information to allow the Firm to meet any reporting obligations under any applicable laws; and (ii) all necessary assistance as required by the Firm to remedy and mitigate the effects and damages resulting from such breach.

## 9. International Data Transfers

Holland & Knight is an international organization with offices in Algeria, Colombia, Mexico, the United Kingdom and the United States. Although our Information Technology systems are located in the United States, Firm personnel may reside anywhere we have physical offices, including countries outside the United States and may remotely access data from any location with internet access.

Firm personnel should avoid transfers of Sensitive Private Information and Special Category Information with respect to Firm personnel or client-rated persons residing in jurisdictions other than those in which the Firm has physical offices. Please contact privacy@hklaw.com for assistance.

Clients and service providers to clients should ensure that any transfers of PI will comply with all relevant privacy and data protection laws, including the General Data Protection Regulation (GDPR). In the event you transfer PI of individuals in the European Economic Area (EEA) to jurisdictions outside the EEA, you must ensure that either:

- There is in force a European Commission adequacy decision that the country or territory to which the transfer is to be made ensures an adequate level of protection for processing of PI; or
- The parties involved in the transfer of PI execute the standard contractual clauses approved by the European Commission decision for the transfer of Personal Data to processors established in third countries from time to time.

## 10. Digital Matter File

Digital data associated with a client representation can most effectively be managed in accordance with the Firm's legal, ethical and contractual duties when it is maintained in a centralized data repository organized on the basis of client matter number, such as the Document Management System (DMS) client matter workspace. We refer to this strategy as the Digital Matter File, a key component in addressing important client relationship management and risk management objectives of the Firm. Because of our heightened duties with respect to data that contains SPI, PHI or SCI, it is all the more important to manage this data consistent with the Digital Matter File strategy.

Digital data associated with a client representation should be created, maintained, shared and transmitted using only Firm applications, accounts and devices that can be configured to allow for organization of the data based on client matter number, in a manner that facilitates associating it with the Digital Matter File.

## 11. Data Loss Prevention (DLP)

The Firm's Data Loss Prevention (DLP) program is designed to prevent data from being shared, used or accessed beyond its intended and appropriate audience or purpose. The DLP program incorporates technical, administrative and procedural safeguards in addressing these issues. By following the guidance in this Policy, you are actively participating in and supporting the Firm's DLP program.

## 12. Contact Information

The Firm has appointed the following contact in the event you have any questions about our privacy practices or this Policy:

Diane Del Re, Privacy and Compliance Senior Manager
Holland & Knight LLP
524 Grand Regency Blvd. | Brandon, Florida 33510
Office 813.901.4196 | Mobile 813.997.7584
diane.delre@hklaw.com | privacy@hklaw.com

## 13. Responsibilities and Revisions

From time to time, we may make changes to this Policy. Any changes will be posted on this page with an updated revision date. If we make any material changes to this Policy, we will notify you by means of a prominent notice on our Sites prior to the change becoming effective. This Policy will be reviewed annually and updated, as necessary. The Firm's General Counsel is responsible for maintaining, reviewing and updating this Policy.

### Revision History

| Version | Date Reviewed | Date Approved | Document Owner | Description |
|---|---|---|---|---|
| 1 | 11.28.2022 | 11.28.2022 | Diane Del Re | Data Protection Policy (Original) |
| 2 | 01.01.2023 | 01.01.2023 | Diane Del Re | Revised and Approved |
| | | | | |