Protecting Personal Identifying Information

Last Updated
March 4, 2025

As a travel advisor, you will handle sensitive customer information on a daily basis, including Personal Identifying Information (PII). Understanding what constitutes PII and how to protect it is crucial for maintaining trust with clients and staying compliant with legal and industry regulations.

What is PII?
Personal Identifying Information (PII) refers to any data that can be used to identify a specific individual. Examples of PII you might handle as a travel advisor include:

- Full names
- Addresses (home and email)
- Telephone numbers
- Social Security numbers (in rare cases, for visa or government-required forms)
- Passport numbers
- Payment information (credit card details, etc.)
- Dates of birth
- Personal travel preferences (which may reveal sensitive information like health conditions)

Protecting PII is essential to prevent identity theft, fraud, and other malicious activities that could negatively impact your clients and your business.

Why Protecting PII is Important

- **Legal Requirements**: Many countries have strict privacy laws, such as the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act (CCPA) in the U.S., that require businesses to safeguard personal data.
- **Trust and Reputation**: Your clients trust you with their sensitive information, and a breach of that trust could lead to loss of business, legal penalties, and a damaged reputation.
- **Security Threats**: Hackers and cybercriminals actively target businesses that handle sensitive information. Even a small oversight can lead to a data breach.

How to Protect PII

1. *Limit Data Collection*- Only collect the PII necessary for booking and planning travel. Avoid asking for additional information that is not relevant to the services you are providing. For instance, if you do not need a client's Social Security number, do not ask for it.
2. *Secure Storage* - Store PII in secure, encrypted systems. Avoid storing sensitive data in unencrypted or easily accessible formats (e.g., plain text documents or spreadsheets). If you need to keep physical copies, ensure they are locked in a secure location.
3. *Use Strong Access Controls* - Limit access to PII to only those employees who need it to perform their job. Implement role-based access controls so that sensitive information is only accessible to authorized personnel.
4. *Encrypt Data* - Ensure that all sensitive information, especially payment details and passport numbers, are encrypted during transmission and at rest. Use secure communication methods (e.g., encrypted email or secure web forms) when sharing sensitive information with clients or third parties.
5. *Regularly Update Software* - Use up-to-date antivirus software, firewalls, and other security tools to protect against malware and hacking attempts. Regularly update your systems and software to patch known vulnerabilities.

Protecting Passwords

A key aspect of protecting PII is safeguarding your passwords. Strong password management is essential for preventing unauthorized access to client data.

1. *Use Strong Passwords* - Ensure that all passwords used to access systems with client data are strong. A strong password should:
    - Be at least 12-16 characters long.
    - Include a mix of uppercase and lowercase letters, numbers, and symbols.
    - Avoid using easily guessable information like your name, the word "password," or sequential numbers (e.g., 123456).
2. *Enable Two-Factor Authentication (2FA)* - Whenever possible, enable two-factor authentication on all systems. 2FA adds an extra layer of security by requiring not only a password but also a secondary verification step (e.g., a text message or authentication app).
3. *Use a Password Manager* - A password manager can help generate and store complex passwords, ensuring that you don't need to remember multiple strong passwords. Password managers store passwords in an encrypted vault and make it easy to use unique passwords for different accounts.
4. *Avoid Reusing Passwords* - Never use the same password across multiple systems, especially for accounts that store sensitive information. If one account is compromised, all others that share the same password will be vulnerable.
5. *Change Passwords Regularly* - Regularly change passwords, especially if you suspect a breach or if an employee leaves your company.

Conclusion

Handling PII responsibly is a critical aspect of your role as a travel advisor. By following best practices for data protection and password security, you can help safeguard your clients' information and maintain their trust. Stay vigilant, stay secure, and always prioritize the privacy of your clients.