IIANC Data Protection Policy

Context and Overview

Key Details

- Policy Prepared By: Adam Petrey & Natalie Simpson
- Approved by Management: 11/25/2020
- Policy Became Operational On: 12/01/2020
- Next Review Date: 12/01/2021

Introduction

The Independent Insurance Agents of North Carolina ("IIANC" or "the company") needs to gather and use certain information about individuals and organizations that it conducts business with regularly.

These can include members, customers, suppliers, business contacts, employees, and other people the organization has a relationship with or may need to contact.

This policy ensures IIANC:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Policy

This Data Protection Policy outlines how personal data for these individuals and organizations must be collected, handled, and stored to meet the company's data protection standards and to comply with the law. These rules apply regardless of whether data is stored electronically, on paper, or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Policy is underpinned by the following important principles which say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the organization (with the exception of public information including name, job title/role, address, phone and email)

People, Risks and Responsibilities

Policy Scope

This policy applies to:

- The office of IIANC
- All staff and volunteers of IIANC
- All contractors, suppliers and other people working on behalf of IIANC

It applies to all data that the company holds relating to identifiable individuals and organizations, even if that information technically falls outside of the Data Protection Policy. This can include, but is not limited to:

- Names of individuals/organizations
- Postal addresses for business and home
- Email addresses
- Telephone numbers (work, cell, home)
- Website address
- Job title/role
- Insurance license(s)
- National Producer Number
- Salary
- Birth Date
- Identified Gender
- Race
- Veteran Status
- Disability
- Any Government issued identification numbers

Data Protection Risks

This policy helps to protect IIANC from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how IIANC uses data relating to them.
- Reputational damage. For instance, IIANC could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with IIANC has some responsibility for ensuring data is collected, stored, and handled appropriately. Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The Chief Executive Officer is responsible for:
    - Ensuring that IIANC meets its legal obligations for data collection and usage.
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Addressing any data protection queries from journalists or media outlets like newspapers.

- The Chief Financial Officer is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

- The Vice President of Marketing is responsible for:
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the IIANC staff covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data IIANC holds about them (also called ‘subject access requests’).
    - Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.

- Approving any data protection statements attached to communications such as emails and letters.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- IIANC will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
    - In particular, strong passwords must be used and they should never be shared. Staff will use and comply with IIANC's password management software.
    - Personal data should not be disclosed to unauthorized people, either within the company or externally.
    - Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
    - Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Chief Financial Officer or Vice President of Marketing.

When data is stored on paper, it is kept in a secure place where unauthorized people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files will be kept in a locked drawer or filing cabinet.
- Employees will make sure paper and printouts are not left where unauthorized people could see them, like on a printer.
- Data printouts will be shredded and disposed of securely when no longer required.

When data is stored electronically, the following steps will be taken in an effort to protect it from unauthorized access, accidental deletion and malicious hacking attempts:

- Data will be protected by strong passwords that are changed regularly.
- Data will not be stored on removable media (like a USB drive or external hard drive).
- Data will only be stored on designated drives and servers and will only be uploaded to approved cloud computing services.
- Servers containing personal data will be stored in a secure location away from general office space.
- Data will be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- All servers and computers containing data will be protected by approved security software and a firewall.

Data Use

Personal data is of value to IIANC. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft:

- When working with personal data, employees will ensure the screens of their computers are always locked when left unattended (while at IIANC office or working remotely).
- Personal data should not be shared informally. In particular, it will never be sent using a non-IIANC owned computer or staff members' personal email, due to security risks.
- Data must be encrypted before being transferred electronically. The Chief Financial Officer can explain how to send data to authorized external contacts.
- Employees will not save copies of personal data to their personal owned computers. Employees will always access and update the central copy of any data.

Data Accuracy

IIANC will take reasonable steps to ensure data is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff will not create any unnecessary additional data sets.
- Staff will take every opportunity to ensure data is updated. (i.e. By confirming a customer's details when they call and conducting an annual data update process.
- IIANC will make it easy for data subjects to update the information IIANC holds about them (i.e. Via the secure company website).
- Data will be updated as inaccuracies are discovered. (i.e. If a customer can no longer be reached on their stored telephone number, it should be removed from the database).

Subject Access Requests

All individuals who are the subject of personal data held by IIANC are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed on how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.
- Request that their personal data be deleted.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made submitted via email to the IIANC Data Analytics Manager at membership@iianc.com. A standard request form is not required but can be provided. The Data Analytics Manager will provide the relevant data within 14 days and will always verify the identity of anyone making a subject access request before releasing any information.

Disclosing Data for Other Reasons

In certain circumstances, the law allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, IIANC will disclose the requested data. However, the Data Analytics Manager will ensure the request is legitimate, seeking assistance from IIANC management and from the company's legal advisers where necessary.

Providing Information

IIANC aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, IIANC has a Privacy Policy which outlines how data relating to individuals is used by the company. The Privacy Policy is available on request. A version of this policy is also available on the company's website.