Zoe Community

GDPR

June 2019

Contents

Privacy Notice

1. What is GDPR ?

- The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and is designed to harmonise
- data privacy laws across Europe.
- Your privacy is important to Zoe Community and we take our responsibility regarding the security of your personal data very seriously.
- We are committed to protecting your personal data, as well as, being transparent about the information we store and collect about you and what we do with it.
- We aim to ensure that, when processing personal data, we will use that data lawfully, fairly and transparently; only for the purpose it was originally collected for, and we will request only data that is relevant and necessary.
- We will endeavour to ensure such data is accurate; is only kept for as long as is necessary and otherwise permanently deleted, and kept secure and confidential.

2. Our grounds for processing your personal data

- Zoe Community may rely on a number of legal bases for collecting personal data
- Our legal bases for processing your data are usually 'legitimate interests'. By 'legitimate interests' we mean for a genuine purpose, necessary for the smooth running of the organisation, and not invasive to your privacy. For all other purposes we will ask for your clear and affirmative consent before processing your details.
- If you are appointed to a specific role within the life of the organisation we may publish your details or share them so members and other relevant individuals/ organisations can contact you. This will cease when you step down from the role.
- We may post photographs and/or video taken at organisation events on our website.
- We will not share your information with any other third parties without your permission unless we have a legal obligation to do so.

3. Reasons why we collect personal data

- To keep you informed about the organisation and about planned events or activities in which you might have an interest.
- For the submission of donor information as part of the Charitable Donations Tax scheme.
- Zoe Community is multi-cultural and may hold different events during the course of the year. You may have provided your personal details on a contact card. This information will only be used in the planning of events which we hope you will be available to attend.

4. Who will use your personal data?

- Unless we inform you otherwise Zoe Community will not transfer or disclose your personal data to any other party. Zoe Community undertakes not to obtain personal data on any individuals from any source other than the person themselves.

5. The principles which will be applied by Zoe Community in relation to the processing of personal data

- Your personal data shall be processed lawfully, fairly and in a transparent manner. At the time of providing personal information, you will be made aware of
  - Who is collecting your personal data
  - Why we are collecting your personal data
  - Who will have access to your personal data
- Your data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Zoe Community will ensure that you are aware of the reason why the personal data is being collected and furthermore you will be assured that Zoe Community will not use the data for any other purpose without your prior consent.
- Zoe Community will conduct periodic reviews to ensure that relevant data is kept accurate and up-to- date.
- Zoe Community will ensure that your personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they were originally collected. Data which is not relevant to such processing will be deleted / destroyed.

- Zoe Community will keep your personal data in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the personal data was collected.
- In preparation for GDPR Zoe Community will prepare a data map of all the personal data that is expected to be collected. The data map will include both soft and hard copy data. The data map will be reviewed periodically to ensure that personal data is kept for no longer that is required. Once the period of use has elapsed, the data will be permanently deleted or destroyed.

6. Where the understanding of consent by the data subject may be in doubt

- Where a person by reason of his or her physical or mental incapacity or age, is or is likely to be unable to appreciate the nature and effect of giving consent, such consent may be given by a close relative.
- Parental consent will be obtained where personal data is to be held for children under the age of 16.
- Consent to continue to hold the personal data will be obtained from the child when he/she reaches the age of 16. Where consent is not obtained personal data will be permanently deleted.
- When relying on consent from a child, we will ensure that the child understands what they are consenting to, the reasons why we are holding their personal data and their rights under GDPR.

7. Personal data held in respect of donations

- Donor details and donations will be are recorded and stored on password protected excel files.
- Donations will be aggregated annually and where the donor has completed a Revenue Enduring Certificate, an online application may will be made on the Revenue ROS website for a tax refund which if approved will be paid directly into the Zoe Community bank account.
- Under Revenue rules Zoe Community is required to retain donor information in respect of tax refunds for a period of 6 years. Donor data which is either not required in respect of tax refunds or which has been retained on file for 6 years will be permanently deleted.

- Donations will be recorded for audit purposes and retained on a donor database. If you do not wish to have your details stored on our donor database please email us at the contact address below.

8. Personal Public Service Numbers (PPSNs)

- PPSN's are recorded by donors on an Revenue Enduring Certificate.
- The Revenue Enduring Certificate will be used solely by Zoe Community for the Charitable Donations Scheme.
- Revenue Enduring Certificates will be stored securely in a locked archive box until due for destruction as outlined above.
- PPSN numbers will not be held in digital format.

9. Your rights in respect of your personal data

- You have the right to obtain from Zoe Community confirmation as to whether or not personal data concerning you is being processed, and, where that is the case, access to the personal data. Our subject access policy which is available on request will provide further detail for you.
- You have the right to obtain from Zoe Community without undue delay the rectification of inaccurate personal data concerning you.
- You have the right to obtain from the controller the erasure of personal data concerning you without undue delay
- You have the right to restrict Zoe Community from processing your personal data
- Zoe Community shall communicate any rectification or erasure of personal data or restriction of processing carried out in respect of your personal data
- You have the right to receive the personal data concerning you in a concise, transparent, intelligible and easily accessible form.
- You have the right to object, on grounds relating to your particular circumstance at any time to the processing of personal data concerning you by Zoe Community
- You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you
- You have the right to lodge a complaint if you are unhappy with the processing of your personal data with the Data Protection Commission.

10. Data Retention

- Zoe Community undertakes not to retain personal data for any longer than is necessary. As a company, we are required to retain certain records, usually for a specific amount of time. Examples of these records are documents containing personal data that is collected for the Charitable Donations Scheme.

- Zoe Community will monitor and identify records that have met their required retention period and arrange their deletion or destruction.

11. Data Security

- Zoe Community will employ high standards of security to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by Zoe Community. Access to personal data is limited to staff members who have appropriate authorisation and password access.

12. Cookies

- Our website will only use essential cookies which are necessary to provide you with the information that is available on our website.
- Our website does not automatically capture or store personal information during use unless you sign up for an event or activity or to receive communications from Zoe Community.

13. Changes to the privacy statement

- Any changes to this Privacy Statement will be posted on this website so you are always aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it.

- If at any time we decide to use Personal Data in a manner significantly different from that stated in this website Privacy Statement, or otherwise disclosed to you at the time it was collected, we will notify you by e-mail, and you will have a choice as to whether or not we use your information in the new manner.
- We will post this Privacy Notice on our website.
- This privacy policy only covers Zoe Community website. Links within this site to other websites are not covered by this policy.

14. Questions

If you have any questions regarding the above statement please contact us at ??????????
We undertake to respond to your query within 48 hours.

Subjects Rights & Access Policy

You, the data subject, have data protection rights that you can exercise over the information you give us. These rights include:

- **to be informed** how your data is being used;
- **to have access** to the information we hold about you;
- **to have inaccuracies corrected**;
- **to have your information erased**; **to object to or restrict** to how we process your information;
- **to not be subject to decisions made by automated processing including profiling**, and;
- **data portability** (to receive your digital information in a useful format).

Under GDPR you have the right to obtain from Zoe Community confirmation as to whether or not personal data concerning you is being processed, and, where that is the case, access to the personal data.

This applies to all types of information - for example, written details about a person held electronically or on paper, photographs and CCTV images.

You are also entitled to know where the information was obtained, how it has been used and if it has been passed on to anyone else.

You have the right to ensure our use of your data is lawful, and that the data we hold is accurate.

If you would like to access the data we process about you, please write to:

Data Protection Leader
Zoe Community
7 Glenbrae Court
Shankill
Dublin 18

or by email to

admin@zoecommunity.ie

The charity is entitled to ask for evidence of identity and to charge a fee, but this cannot exceed €6.35. However we will not charge for this service unless you make multiple requests within a short space of time.

Data Retention Policy

1. Data Retention

As a company Zoe Community is required to retain certain records, usually for a specific amount of time. Under GDPR we have a statutory obligation to only keep records for the period required. Zoe Community shall not retain any personal data for any longer than is necessary for the purpose(s) for which that data was collected, held, and processed.

When establishing and/or reviewing retention periods, the following shall be taken into account:

- The type of personal data in question;
- The purpose(s) for which the data in question is collected, held, and processed;
- The Company's legal basis for collecting, holding, and processing that data;
- To whom the data relates e.g. age of the data subject

If a precise retention period is not fixed for a particular type of data by law, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

Certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Organisation to do so (whether in response to a request by a data subject or otherwise).

2. Data Portability

Subjects have the right to obtain and reuse personal data for their own purposes across different services. Zoe Community will facilitate subjects in the movement, copying or transfer of personal data from one IT environment to another in a safe and secure way, without affecting its usability. Any such action will be only be undertaken with the express written instruction of the data subject which will include the agreed manner in which the data will be moved, copied or transferred. Notwithstanding such action, personal data which continues to be held by Zoe Community will be subject to the Data Retention Policy.

3. Key Responsibility

The destruction of redundant personal data is a rolling obligation. As time passes data will be eligible for destruction due to the expiry of time i.e. 6 years for charitable donations or as children reach the age of 16 and are then required to provide explicit consent where previously the data was held on behalf of the parent / guardian.

The challenge in the management of data retention is to establish a periodic discipline whereby eligible data will be identified for destruction and then destroyed. Data retention records will be updated to record destruction for record purposes.

Our Data Protection Leader is responsible for identifying the documents that must or should be retained and determining the proper period of retention. The responsibilities of the Data Protection Leader include:

- Arranging for the proper storage of records
- Handling the destruction of records whose retention period has expired.
- Planning, developing and prescribing document disposal policies, systems, standards and procedures.
- Establishing standards for filing and storage equipment and recordkeeping supplies.
- Periodic review of the data retention schedules
- Planning the timetable for the annual records destruction exercise and the annual records audit.
- Evaluating the overall effectiveness of the data retention process.

4. Implementation

Upon the expiry of the data retention period or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

Hard copy documents
Hard copy records must be stored in a safe, secure and accessible manner particularly those that must be retained for regulatory or statutory reasons.
Documents containing confidential or personal information should be disposed of either by shredding or by using confidential waste bins or sacks.

Personal data in paper form should not be disposed of waste paper – records containing personal data or special categories of information should be securely shredded before being disposed of.
Hard copy documents which cannot be safely disposed of or destroyed offsite should be brought to the Organisation for destruction

Soft copy documents
Electronic data including email, social media pages and digital files should be deleted so as to be put beyond use. Note that archiving will not delete data. It will often be sufficient simply to delete the information, with no intention of ever using or accessing it again, despite the fact that it may still exist in the electronic ether.
Deletion can also be effected by using one of the following methods of disposal:-

- Using secure deletion software which can overwrite data;
- Using the function of "restore to factory settings" (where information is not stored in a removable format);
- Sending the device to a specialist who will securely delete the data.

Individuals should not keep copies of personal data records at their homes once the original records have been destroyed. It should be remembered that Zoe Community is the Data Controller, carrying ultimate responsibility for the storage, security and retention of the data.

5. Procedure

Why the procedure

- This procedure must be followed to ensure that the Data Retention policy is implemented and can be evidenced accordingly

Who does the procedure apply to

- The procedure must be followed by anybody who holds personal data on behalf of Zoe Community

When must the procedure be followed

- Personal data held must be reviewed at least annually

Where should the procedure be undertaken

- The review can be conducted at the discretion of the data holder at their choice of location or onsite at the Organisation under supervision of the Data Protection Leader.

What is the procedure ?

- It is the responsibility of the data holder to ensure that the procedure is followed
- Personal data must be examined to ascertain whether the data must continue to be held on behalf of Zoe Community
- Digital files should be permanently erased. Ensure that deleted files are also removed from the Recycle folder.
- Hard copy data should be shredded or destroyed beyond identification.
- The destruction of paper by burning is not recommended.
- The data retention records should provide evidence of
    - The time of review of the personal data
    - What personal data was reviewed
    - Where the personal data was stored
    - The data selected for destruction
    - The manner in which the data was destroyed
- The Data Protection Leader will record the details of the data destroyed in the format below on the office desktop

Data	Data Storage Location	Description of Data	Method of destruction	Person evidencing destruction

Volunteer Policy

1. Purpose

Our volunteer policy has been created to show our volunteers and potential volunteers that we have spent time and care in planning how volunteers will be welcomed at Zoe Community. It states that volunteers will be treated in a fair and consistent way and will assist our volunteers in understanding what support is available to them and what they can expect from the Organisation.

- This policy has been produced to provide guidance on the role of volunteer
- It aims to ensure that there is a positive and mutually beneficial volunteering arrangement and that volunteers are properly appointed and receive the appropriate amount of direction from the Organisation
- The policy also provides clarity around the responsibilities of volunteers and also guidelines for the management around any risks or issues that may arise.

2. Scope

- This policy applies to all volunteers who participate in the activities of the Organisation
- Volunteers must be minimum age of 18
- Garda Vetting must be successfully obtained where a volunteer wishes to participate in activities requiring same

3. Principles

Zoe Community recognises the commitment of volunteering and will endeavour to ensure that the volunteer will:

- be offered appropriate training
- receive supervision and support
- know who to go to if there is a problem
- be reimbursed for approved out-of-pocket expenses incurred on behalf of the Organisation
- be made aware of any disciplinary and grievance procedures

- be treated fairly and not experience discrimination of any kind
- have safe working conditions, including insurance cover

4. Insurance, health and safety, accidents and risk assessment

Zoe Community has a public liability insurance policy so that volunteers are covered by public liability insurance. It covers all the activities which the Organisation will organise. Health and Safety considerations are central to all of our activities both on site and at other venues. We keep our Health and Safety Policy in mind and we will provide instructions on how to perform tasks safely.

5. Volunteer Management Procedures

We will endeavor to ensure that Zoe Community makes your volunteering experience an enjoyable and meaningful one.
Our commitments to you are as follows:

- Volunteer records will be accorded the same confidentiality as staff records.
- Zoe Community respects the right of volunteers to privacy and confidentiality. In turn, volunteers are responsible for maintaining the confidentiality of all privileged information to which they are exposed to while volunteering.
- Volunteers will have access to space, equipment and facilities necessary to effectively fulfil their duties.
- Volunteers are requested to uphold the standards of the Organisation in their behaviour and dress while performing their duties

6. Volunteer Selection

Volunteers may be requested to provide a C.V. or a reference.

- Suitable candidates will be invited to have an informal chat to ascertain their interest in and suitability for the role.
- For certain activities prior Garda vetting clearance will be required before the volunteer can commence duties.

- Volunteer appointments are made only after the role description has been agreed and the appointment process has been completed.
- Volunteers will be given a clear and accurate description of the tasks and responsibilities that are agreed upon
- The role description may be amended in joint agreement between the volunteer and the organisation.

7. Volunteer Supervision and Evaluation

- Volunteers will be provided with a clearly identified contact person within the organisation who will be responsible for their day-to-day management.
- If a volunteer is unable to attend at a scheduled location, we would ask that contact person is informed as early as possible so that alternative arrangements can be made.
- Volunteers and their contact persons should meet periodically to discuss their duties
- Volunteers who do not adhere to the policies of the Organisation may be subject to dismissal. Whilst no contractual arrangement is in place we will adopt staff dismissal procedures to ensure that the rights of the individual are fully respected.
- Volunteers must seek prior approval from their contact person before undertaking or submitting to any activity which might significantly affect the Organisation. This includes, but is not limited to, statements to the press, joint initiatives with other bodies, or agreements involving contractual or financial obligations.
- If a volunteer feels they are being unfairly treated, they should discuss the matter with their contact person.

Security & Own Device Policy

1. Security Policy

Zoe Community will employ high standards of security to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by Zoe Community. The

security policy will apply to all persons that are specifically approved to hold personal data on behalf of the Organisation.

Once we receive your data, we use appropriate technical and physical security measures, including anti-virus protection to protect your personal data, from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure.

An overview of the key areas:

- Office Administration digital files are password protected on the office desktop
- Personal data is stored in Salesforce (or alternate CRM, if SalesForce is not available immediately)
- Access to personal data in Salesforce is restricted and subject to password protection.
- Hard copy records are kept in locked cabinets or locked boxes in the office or attic
- Digital storage devices are password protected
- Other than our personal data records that must be kept indefinitely for legal compliance we will remove your information from our systems no less than six years after your last personal contact
- Personal data obtained on a once-off basis will be deleted when the requirement to hold the data ceases
- CCTV footage if used will be erased on expiry of 4 weeks after recording.

2. Data Security

Zoe Community will employ high standards of security to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by Zoe Community. Access to and management of personal data records is limited to Zoe Community management who have appropriate authorisation and password access.

Zoe Community' records will be stored in a safe, secure and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site.

3. Security

To prevent unauthorised access to all Zoe Community and own computers/devices containing personal data must have password protection. Passwords must have a minimum of 8 characters including a combination of upper and lower case and including at least 1 number.

- Password should ideally be reset every 12 weeks.
- Devices should self-lock if left idle.
- Organisation owned desktops and laptops should only use applications / software necessary for the completion of duties.

4. Use by employees and authorised volunteers/leaders of their own devices in the processing of personal data

In recognition of the participation by volunteers and leaders in the processing of personal data the Board of Directors have adopted a Bring Your Own Device Policy so that the GDPR policy extends to all devices used in the processing of personal data by authorised volunteers and leaders.

This policy is intended to protect the security and integrity of personal data and the IT systems in operation.

I. Acceptable Use

- Zoe Community defines acceptable business use as activities that directly or indirectly support the activities of the organisation
- The company defines acceptable personal use during opening hours as reasonable and limited personal communication or recreation.
- Employees may be blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company.
- Devices' camera and/or video capabilities should not be used on site.
- Organisation owned devices may not be used at any time to:
  - Store or transmit illicit materials
  - Engage in activities which are not consistent with the mission of the Organisation
- Zoe Community prohibits staff from texting or emailing while driving and only hands-free talking while driving is permitted.

- Laptops , smartphones and tablets used onsite or offsite in respect of Organisation duties or activities must be from recognised manufacturers
- Reimbursements of any costs in respect of a personal device is subject to prior Board approval
- All devices used inside the Organisation should have appropriate protection from viruses etc.

II. Risks/Liabilities/Disclaimers

- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the Office Administrator within 24 hours.
- Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and to adhere to Organisation policies.
- Severe penalties can apply under the GDPR legislation. Disciplinary action may be taken where this policy is not complied with.

5. Procedure

Why the procedure

- This procedure must be followed to ensure that the Security and Own Device Policy is implemented and can be evidenced accordingly

Who does the procedure apply to

- The procedure must be followed by anybody who holds or has access to personal data on behalf of Zoe Community

When must the procedure be followed

- Security around personal data applies at all times

Where should the procedure be undertaken

- In all places and across all devices / equipment where personal data is held

What is the procedure ?

- Data held in the Office
    - Office Administration digital files must be password protected on the office desktop
    - The password should contain a mix of numbers & letters including at least one higher case letter.
    - Personal data is stored in Dropbox (until Sales Force becomes available) Access to personal data in Dropbox is restricted and subject to password protection.
    - Hard copy records are kept in locked cabinets or locked boxes in the office
    - Digital storage devices are password protected
    - Some personal data records may have to be kept indefinitely for legal compliance
    - Where there has been no contact with the data subject for 6 years , personal data held will be permanently deleted.
    - Personal data obtained on a once-off basis will be deleted when the requirement to hold the data ceases

- Data held in the Organisation
    - CCTV footage will be erased on expiry of 4 weeks after recording

- Data held outside the Organisation
    - Passwords should be changed periodically
    - The password should contain a mix of numbers & letters including at least one higher case letter.
    - Hard copy records should be kept in a secure area to avoid loss or theft

Files on digital storage devices should be password protected using a mix of numbers & letters including at least one higher case letter.

Third Party Contracts

Review of third parties providing services or contracts used by Zoe Community in which personal data is processed.

The review covers the legal jurisdiction in which the operational activities of the third party are located and the disclosed status of compliance with GDPR rules.

The General Data Protection regulation is a set of laws due to be enacted in the EU in 2018. Privacy Shield is an agreement between the EU and US allowing for the transfer of personal data from the EU to US.

The GDPR has specific requirements regarding the transfer of data out of the EU. One of these requirements is that the transfer must only happen to countries deemed as having adequate data protection laws.

In general the EU does not list the US as one of the countries that meets this requirement. Privacy Shield is designed to create a program whereby participating companies are deemed as having adequate protection, and therefore facilitate the transfer of information. In short, Privacy Shield allows US companies, or EU companies working with US companies, to meet this requirement of the GDPR.

However a distinction is being drawn around the use of services or systems of third parties.

- Are we using an 'industry standard' system to process personal data?
- Do we input personal data into the system?
- Do we allow third party access to our personal data?
- Do we use the services of third parties where we transfer or provide personal data to the third party?

Communication	Financial	Storage	Service Providers
GMail/email through zoecommunity.ie		Dropbox and Salesforce	

Compliance Checklist

Privacy Policy	Responsibility
The data map will be reviewed periodically to ensure that personal data is kept for no longer that is required. Once the period of use has elapsed, the data will be permanently deleted or destroyed	
Consent to continue to hold the personal data will be obtained from the child when he/she reaches the age of 13. Where consent is not obtained personal data will be permanently deleted	
Donor data which is either not required in respect of tax refunds or which has been retained on file for 6 years will be permanently deleted	

Volunteer Policy	Responsibility
Zoe Community recognises the commitment of volunteering without remuneration and will endeavour to ensure that the volunteer will be offered appropriate training	

Data Breach & Notification Policy	Responsibility
If such an incident occurs the following steps should be taken. Immediately inform the Senior Pastor who will then inform the Board Chairman & Company Secretary	

Data Retention - See Privacy Policy above	Responsibility
The challenge in the management of data retention is to establish a periodic discipline whereby eligible data will be identified for destruction, then destroyed and data retention records will be updated to record destruction for record purposes.	

Security & Own Device Policy	Responsibility
Zoe Community' records will be stored in a safe, secure and accessible manner	
Passwords must have a minimum of 8 characters including a combination of upper and lower case and including at least 1 number	