DEVELOPMENT TRUSTS ASSOCIATION SCOTLAND
the community-led regeneration network

SENSCOT LEGAL

GDPR Compliance Health-check

	Yes	No	Actions	Notes and Good Practice
1. Awareness				
Have you raised GDPR at Board level? Are your employees and volunteers aware of the changes?				Raise internal awareness and offer access to training to ensure that all can participate according to their level of responsibility on the principles and the concepts of the GDPR. You should make sure that decision makers and key people are aware of the law. They need to appreciate the impact the GDPR is likely to have. Engage senior management in privacy matters and audits
Have your employees/volunteers accessed in-house or other training on GDPR?				Train, regularly, the employees/volunteers dealing with personal data and on your organisation's policy and procedures for data management and security
Are you a data controller or processor or both?				The Controller processes Personal Data in connection with its business activities. The Processor processes Personal Data on behalf of other businesses and organisations.

	Yes	No	Actions	Notes and Good Practice
2. Data Held				
What personal data is being processed? (e.g. name, address, telephone number etc.)				Personal Data is information that identifies an individual
Why is this personal data processed? For what purpose is it used?				
With the expanded definition of special category of data in mind, is any special category data held or processed If so, for what purpose?				Within the GDPR, the term "special category data" replaces the existing term "sensitive personal data". It also encompasses more data types than the current definition. (e.g. medical/health data, ethnic origin etc.)?
Have you identified a legal basis?				**Note that under GDPR there are 6 lawful bases for processing data – *consent* will NOT automatically be the most appropriate for you. *See Briefing note page 3 for further information***

	Yes	No	Actions	Notes and Good Practice
3. Governance				
How you are planning to update your privacy notices and ensure that the data security process of your service providers/data processors are of a similar standard to yours?				See template privacy notice
Have you assessed whether your organisation requires to appoint a data protection officer (DPO)?				As a small organisation, data protection and GDPR compliance responsibilities sit with the board. You are not required to have a specified DPO, but everyone within the organisation should be aware of GDPR and it is good practice to have a named person who is not a DPO but has an overview of the responsibilities.
If a DPO is required, whom must they report to?				
What is the DPO's responsibilities?				
As a data controller, have you set up the required contract with all of the required terms?				**If a controller uses a third party to process data on their behalf there must a contract in place. The information required in the contract and necessary clauses can be found here: -** **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/**

Have you set up your central record of processing activity as yet?				Data mapping, data protection policy, privacy notice, security breach management process and policy, employee policy, privacy impact statement, asset register, consent records, breach reporting.
Are you aware of the requirement to carry out Data Processing Impact Assessments (DPIA)? Are you aware of when this may be necessary?				You must carry out a DPIA when: using new technologies; and the processing is likely to result in a high risk to the rights and freedoms of individuals. processing that is likely to result in a high risk includes (but is not limited to): systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals. large scale processing of special categories of data or personal data relation to criminal convictions or offences. This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms eg based on the sensitivity of the processing activity. large scale, systematic monitoring of public areas (CCTV).

	Yes	No	Actions	Notes and Good Practice
4. Consent				
If you rely on consent, what measures have you put in place to seek, obtain and record consent and are you aware of the changes you need to make?				Make the consentClear & plain language? Pro-Actively given Document and store it Make it easy to withdraw Consent should be used for processing data for newsletters/mailings etc
Do your activities involve, vulnerable people, children or young people?				How do you obtain consent? Is it necessary to obtain parent, guardian or attorney consent?
Will /you be relying on consent to hold children's data?				Children13 or over are able to provide their own consent otherwise parental consent is needed. The Privacy notice should be in clear and plain language.

	Yes	No	Actions	Notes and Good Practice
5. Storage and Archive				
How does your organisation store data?				Electronic/physical files/laptop/pen-drive/database/cloud/case management/reporting/
If electronic – where is it stored?				Servers? Other software used e.g. mailchimp/survey monkey
Have you identified third party processors?				Where and how is data stored?
If physically held, where is this stored?				If elsewhere, identify the third party holding the data.
Do you archive your data?				Identify the third party holding the data.
If yes, how?				

	Yes	No	Actions	Notes and Good Practice
6. Security				
Describe your security measures in relation to your operations in order to keep data secure?				Physical, administrative and technological measures?
Who has access to data from outwith the organisation?				Cleaners, IT , visitors, customers,
Do you have policies and procedures in place for detecting and/or dealing with breaches? If so, what are they?				See template *breach management policy* and *breach management report*
If you have had a security breach in the past, what actions did you take to remedy and resolve?				
Do you have a mechanism to check that there has been no breaches or unauthorised access to the data held?				
Do you have a process in place for reporting breaches to the ICO?				
How will you communicate this to your staff?				

	Yes	No	Actions	Notes and Good Practice
7. Destruction of Data				
How is data destroyed?				Shredded/deleted
By who?				Agreements? Where? Onsite?
8. Using Service Providers				
Are any processing activities carried out by a third party?				List, describe the processes and location – Payroll etc
Is there a written agreement?				
Have you ascertained what security measures the service providers have in place?				Do they match yours?
9. Transfers of Data				
Do you transfer data across the organisation or to third parties?				Do you transfer data over email or letter to anyone outside of the EU? Do you within your organisation or externally transfer data outside the EU? This would include storage inservers like google drive, icloud or if you use survey monkey, mailchimp?
How?				
In what countries are these third parties based?				
Where data is transferred out of the EEA (European Economic Area) what measures are used to ensure that there are				

adequate protections in place?				