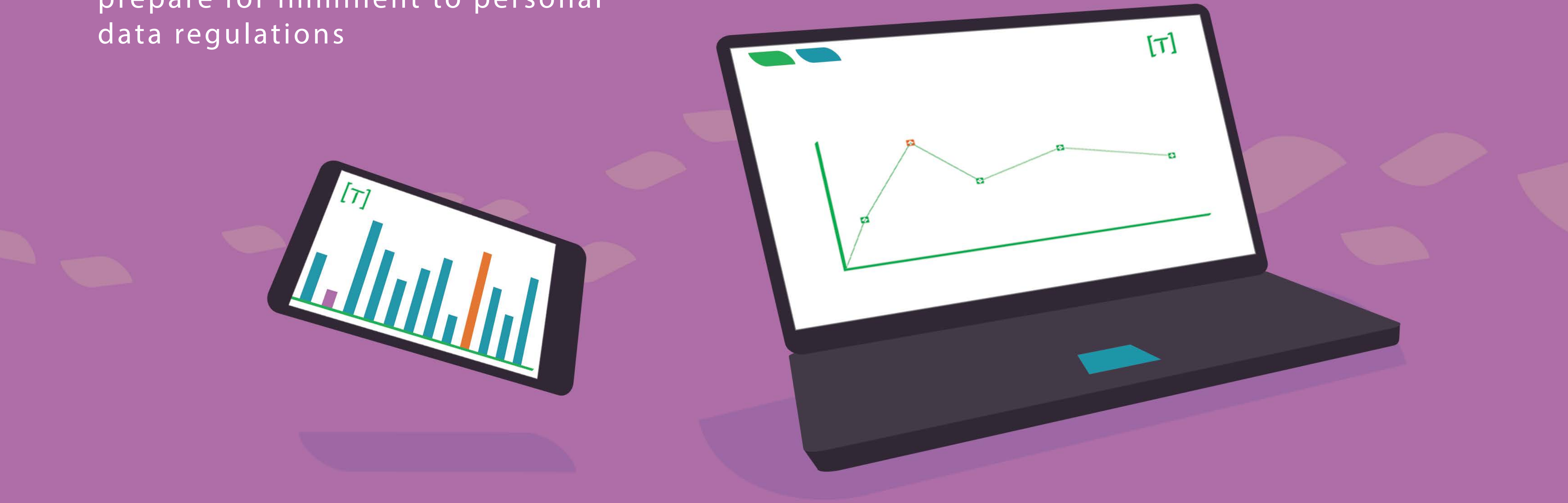
A GUIDE TO GENERAL DATA PROTECTION REGULATION [GDPR]

What charities should do to prepare for imminent to personal data regulations



[Prepared by]
David Melville, Chairman

Transform FOUNDATION

Nick Taylor Managing Director, UKI Strategy

accenture

JAN 2017

[SNAPSHOT]

Introduction

Lots of charities have approached the Transform Foundation over the last year asking us for guidance about how General Data Protection Regulation (GDPR) - the EU's forthcoming regulation on data protection – will impact them and what they need to do to ensure they are compliant. With GDPR coming into force on **May 25th 2018,** these queries have become more and more frequent.

Key contributors

To help address these concerns, we engaged the support of the Managing Director at Accenture that has been leading their work on GDPR. Working with Nick Taylor, we have put this White Paper together as our first response to answer some of the queries we have received.

It provides an explanation of what GDPR is, summarises the key impacts it will have on the charity sector and provides advice on some steps charities can take to be prepared for it.

What is GDPR?

So the GDPR aims to update legislation to make it more applicable to today's world – as the current guidance is dated by some 20 years. It expands the definition of data to include information about us from a physical, physiological, economic, mental, genetic, cultural and social identity perspective – which will have an impact on every charity that takes a donation in some shape or form.

This is a different way of thinking of personal data, as you no longer own the data – the data subject owns their data and as such can make new demands as to what is done with their information. This comes into effect in May 2018, and although that seems a way off, there are a number of activities and measures that need to be in place, requiring action to be taken now.

Why is GDPR relevant to charities?

Personal data is the lifeblood of charities. We deal with the intricacies of life; with organisations for birth, bereavement, bonding, betrayal, blindness, betterment, building, bankruptcy, etc. This being one letter and a small slice of the plethora of support we provide. In this we have people's most intimate details, their personal facts concatenated into the 0's and 1's of our systems, and with the obligation to ensure these are kept secure and are used responsibly.

We have been driving this through our organisations as data protection, but a change is on the way in terms of regulation. This is a good thing – as it ensures that our personal details are ours to own and for companies to provide transparency in how they collect, maintain, process and delete the data we have agreed to provide them.

[REPORTING DATA BREACHES]

72 hour requirement

One of the main changes are that 'data controllers' and 'data processors' are required by law to report a general personal data breach to supervisory authorities within 72 hours. This will put huge emphasis on the role of the data processor(s) - which may be a third party provider (partners, cloud services, out sourced provision, etc.). 72 hours is not a lot of time to understand and communicate the impact given the reputational damage and monetary fines could be significant.

> "Charities that aren't starting to engage with the promise, and threat, of an increasingly digital future run the risk of sleepwalking towards a precipice. Charities planning for the future based on today's circumstances are likely to find themselves not just outpaced by change, but obsolete. Digital technology presents perhaps the greatest threat to today's civil society. but it is also its greatest opportunity, ready to be harnessed by the leaders of tomorrow."
>
> **NPC Report**, Dec 15 2015

Requirement for a DPO

The Regulation requires organisations to implement a wide range of measures to reduce the risk of their breaching the regulations and to prove that they take data governance seriously – with a requirement to put a Data Protection Officer (DPO) in place if you are processing data at scale.

There are more onerous restrictions regarding consent in profiling and decision making using personal data. Controllers have a wider range of obligations around restricting data that is being challenged and informing others using that data that it is restricted.

Transfers of personal data to recipients in "third countries" (i.e. outside of the European Economic Area) continue to be regulated and restricted.

NPC

TECH FOR COMMON GOOD

The case for a collective approach to digital transformation in the social sector

David Bull, Tris Lumley, Farooq Sabri and Ria Bowler
December 2015

[6 KEY IMPACTS TO CHARITIES]

1 Consent

Is likely to be one of the main areas to address as you are likely to have a large amout of personal data that you are storing or processing that you will have to ensure complies to the regulations.

2 Affirmative action to indicate consent

The person must be required to do something to confirm they consent, by submitting a form or ticking a box for specific areas of consent.
The absence of action cannot be used here.

3 Freely given

The person must give their consent without force, ie they have a choice, and do not have to give unnecessary details to undertake the transaction.

4 Informed

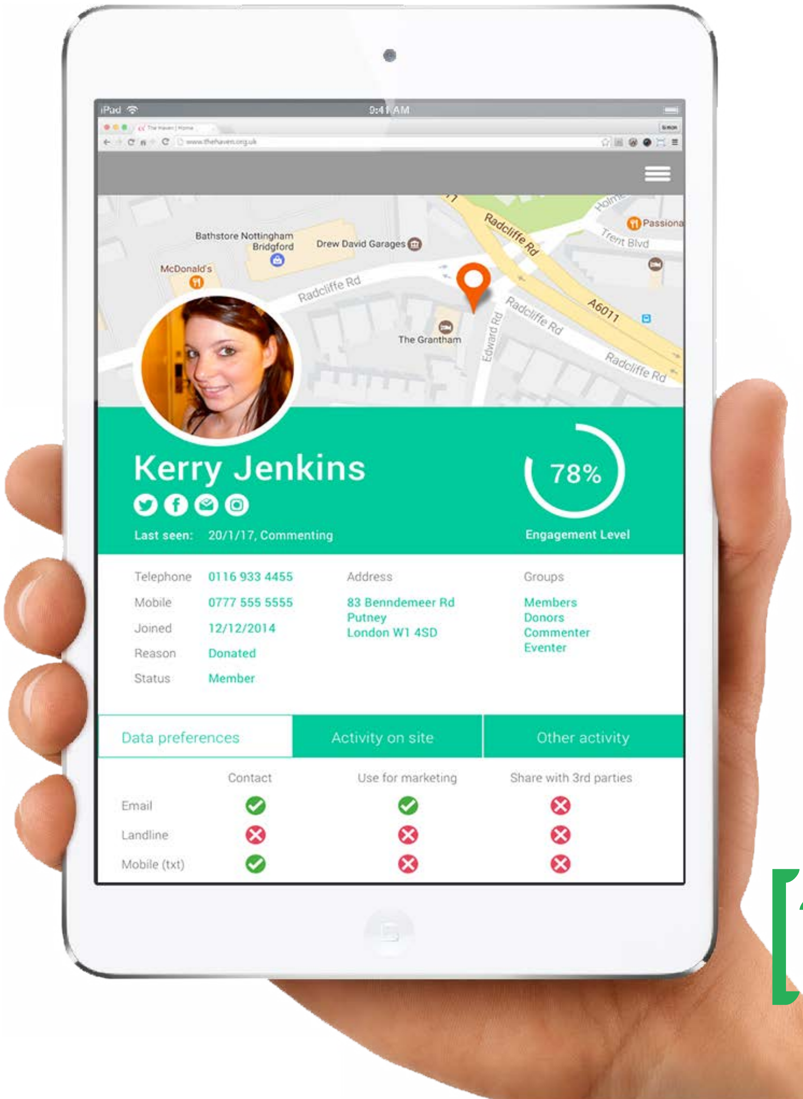
It must be clear to the person exactly what is being asked, why, and how they opt-in or out. Plain English is key.

5 Specific

Related to condition 2, the consent given will be specific to the processing stated at time of consent, and cannot unreasonably be changed later without further consent. Depending on the amount and type of data held, you may have to go back to the owners of the personal data to ensure consent is obtained.

6 Data Management

Is likely to be high in the priority list. Not only what you have and how secure it is, but also what third parties you interact with using personal details and also how to respond to new requests that are part of the regulations.



Kerry Jenkins

78%
Engagement Level

Last seen: 20/1/17, Commenting

Telephone	0116 933 4455	Address	Groups
Mobile	0777 555 5555	83 Benndemeer Rd Putney London W1 4SD	Members Donors Commenter Eventer
Joined	12/12/2014		
Reason	Donated		
Status	Member		

	Contact	Use for marketing	Share with 3rd parties
Email	✓	✓	☒
Landline	☒	☒	☒
Mobile (txt)	✓	☒	☒

[WHAT NEXT?]

6 Practical steps

25th May 2018

Respond to breach in 72 hours ..

.. or 4% income risk

This may seem like a headache or an impossible task, but the way of thinking of this should be an evolution of your business – as being close to your volunteers, beneficiaries or donors is likely the most important aspect of being able to deliver value. The right level of insight and leverage of these details allows you to run and expand your ability to serve them.

The 6 practical first steps in this journey to manage personal information are:

1 Who knows most

- about what personal data you hold and process? Get them to document where it is and how it is used.

2 Understand the processes

- that leverage this data and whether they utilise third parties, cross boarders, drive decisions, etc.

3 Determine the risks

- you may have in using this data – access, security, processors, etc to start to understand the areas you may need help with.

4 Engage a third party

- that has experience in the legal, compliance and other changes required to manage the regulations that are coming through.

5 Develop your approach

- to making the changes, which are likely to be in the spaces of employee understanding, data management, organisation and governance, contracts with third parties, levels of responses to requests, etc.

6 Focus on the biggest risks first

- understand that this is a journey that will evolve over time to become business as usual, where you will always have to keep an eye out for changes in the data you hold and how you manage it.

[IMPACTS TO CHARITIES]

Understanding individuals

There are new rights for the individual to understand, these include:

- What data you hold about them,
- to provide this to them within a set period,
- to demonstrate who sees it,
- how it is used and
- what decisions may be taken with it.

Individuals have the 'right to be forgotten' and a 'right to object' to their details being used, transferred or held.

This makes the control of the data and the interactions you have with third parties key in being able to manage the requests that might be made of you.

Other key points of consideration

There are a number of other areas that will need to be addressed such as:

- Validating who are your data processors and your contracts with them.
- Updating your technology to ensure data is tagged effectively.
- Enhancing your security and governance to deal with breaches, etc.

[CONCLUSION]

A new opportunity

This legislation is coming and this should be treated as an opportunity to look at your organisation to understand what opportunities you may have in not only meeting some compliance criteria – but really understanding your volunteers, employees, beneficiaries, and donors.

These are what makes your organisation thrive and this is the time to get closer to them and enhance the trust you may build with them.