

Better the Devil You Know: Living with GDPR



CAMERON SEMMES STOLL

*Data Protection Officer & Counsel
Blackbaud*

bbcon[®] 2018



HI! Cameron Stoll

TITLE

Data Protection Officer and Counsel

AT BLACKBAUD

2 years

HOMETOWN

Charleston, SC USA

ABOUT ME

I strive to ensure Blackbaud protects the privacy and security of the data of our customers and their donors, so that each can focus on social good! I'm a Certified Information Privacy Professional in EU and US laws and Certified Information Privacy Manager.



AGENDA




GDPR's Impact



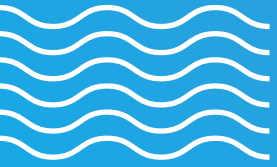
Brexit & GDPR



**Your Future Areas
of Focus**



The following summary does not constitute legal advice and should not be construed as legal opinion or advice on any specific facts or circumstances.



GDPR'S IMPACT

- *How has the GDPR affected organisations?*
- *How has the GDPR affected the global landscape?*



In May 2018, 61% of
charities reported
they were ready for
the GDPR.

*-IOF and Blackbaud's "The Status of UK
Fundraising 2018 Benchmarking Report"*

As a result of GDPR compliance:

53%

Of charity workers say their email database has **decreased by less than half.**

18%

Of charity workers say their email database has **decreased by more than half.**

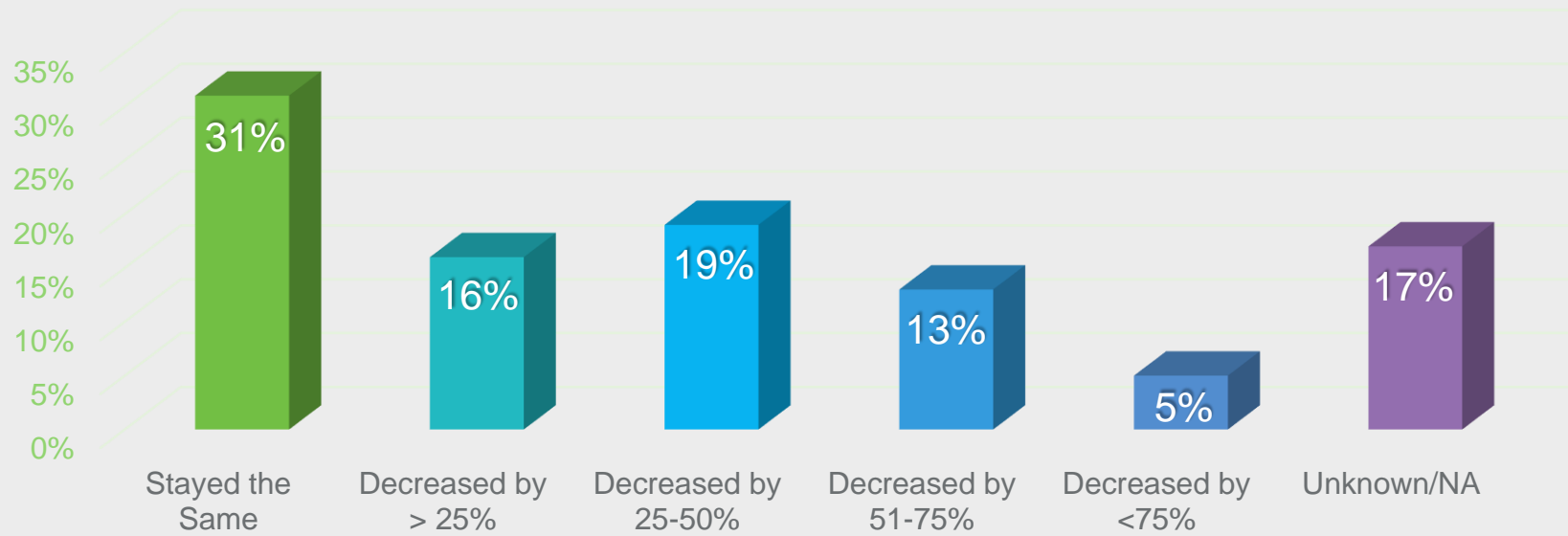
31%

Of charity workers say their email database has **stayed the same size.**

-nfpSynergy and Third Sector's "Post-GDPR Survey"

As a result of GDPR compliance:

Access to Supporters by Email



-nfpSynergy and Third Sector's "Post-GDPR Survey"



GDPR affects even giant FPOs.

Facebook claims it lost **1 million** European monthly active users in the 2nd quarter 2018, “purely due to the GDPR impact”

GLOBAL IMPACT: New or pending laws that mirror GDPR

India

Borrowed some
GDPR principles for
draft Data
Protection Bill

Brazil

Nearly identical
General Data
Protection Law

California

Consumer Privacy
Act has GDPR-like
provisions

Malaysia

Update to laws
could be modelled
after GDPR



BREXIT & GDPR

- *How will GDPR change as a result of Brexit?*
- *Can we still send data to and from the EU?*



Of this we're certain...

- The EU Withdrawal Act will incorporate the GDPR into UK law at the time of exit.
- The UK's Data Protection Act 2018 will remain in place.

**GDPR principles will stay
in tact post-Brexit!**

This is up in the air...

DATA TRANSFER

OPTIONS:

1. Data protection agreement between the EU and UK allowing free flow of data
2. Standard Adequacy Decision
3. Chapter V transfer mechanisms like Standard Contract Clauses, binding corporate resolutions, etc.

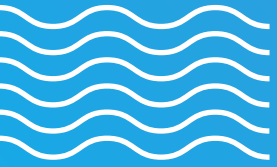
ICO'S PLACE

OPTIONS:

1. Data protection agreement provides that ICO remains in the European Data Protection Board and One Stop Shop
2. ICO out of the EDPB and One Stop Shop. Unable to weigh in on policy.



In the event of No-Deal Brexit, plan for an alternative transfer mechanism to receive data from the EU.

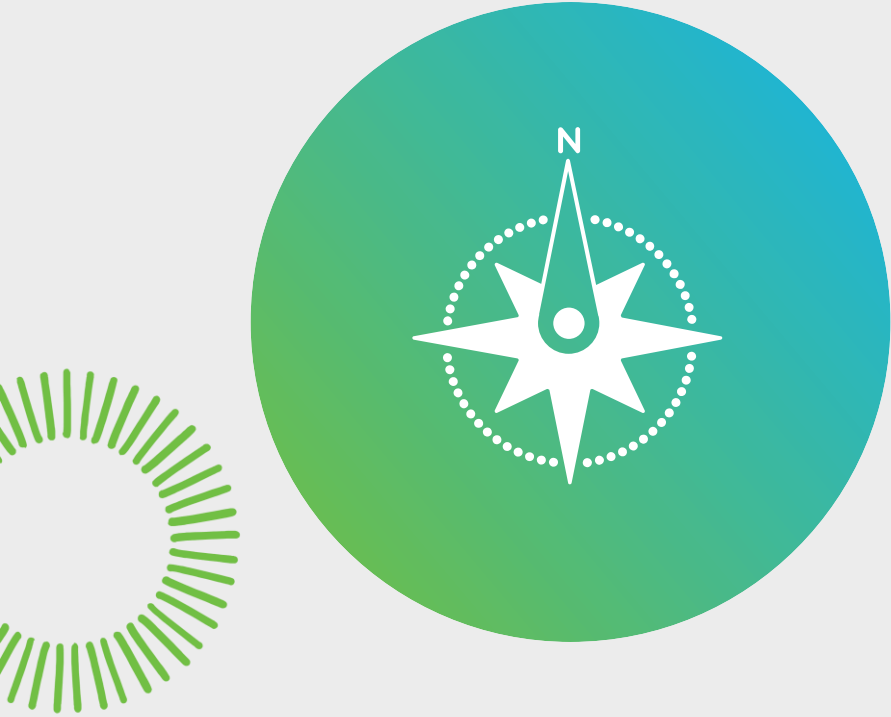


YOUR FUTURE AREAS OF FOCUS

- *What should our programme focus on now?*
- *How will the ICO be enforcing GDPR?*



What should our programme focus on now?



1. **MAINTAIN.** Keep doing the good things.
2. **GAP FILL.** Turn to projects you didn't do well or complete prior to May 25th.
3. **IMPROVE PROCESS.** Use performance data to optimise processes.
4. **REVIEW ICO PRIORITIES.** Double down on areas ICO is making a regulatory priority.

What should our programme focus on now?

Emails

Continue adhering to your email rules. Categorize all new emails (direct marketing, legitimate interest etc.) as they are developed. Honor opt outs. Refresh consents.

New Data Processes

Have a documented process for reviewing all new data uses. Assign legal basis. If required, perform LIA or DPIA. Add to RoPA. Update privacy notices.

Data Subject Rights

Review your processes for respecting data subject rights in light of how your organisation has reacted to those you've received. Are you doing so in a timely manner? Can you make the process more efficient?

Processors

Have a documented process for ensuring all new vendor contracts include Article 28 provisions. Develop robust vendor due diligence process when onboarding vendors and request audit reports (SOCs, PCI) annually.

“

Voluntary compliance is still the preferred route, but we will back that up with tough action where it's necessary. Hefty fines can and will be levied on those organisations that persistently, that deliberately, and negligently flout the law.

ELIZABETH DENHAM, UK INFORMATION COMMISSIONER

”

UK ICO's 2018-19 Regulatory Priorities

IAPP Europe's Data
Protection Intensive
2018, 18 April 2018



Triage projects using ICO's full list of regulatory priorities for 2018-19:

1. Cyber security breaches of financial/sensitive data
2. AI, big data & automated decision making
3. Device tracking for marketing/politics
4. Impacts on children
5. Facial recognition technology
6. Credit reference agencies and data brokering
7. Law enforcement data
8. Right of erasure applications

-ICO's draft *Regulatory Action Policy*, 4 May 2018

ICO's regulatory action will be stronger for data protection violations that are:

Serious and high impact

Intentional or neglectful

Repeated

Involve novel issues or tech

Highly intrusive

Harmful to the public

ICO's regulatory actions under GDPR to date:

0

GDPR fines.

Expect the first to be levied by the end of 2018.

1

ICO enforcement notice, issued against Canadian political engineering firm, AggregateIQ.

6,281

Complaints made to the ICO between 25 May and 3 July.

TO WRAP UP

- GDPR has global impacts and may result in decreased email appeal volume
- GDPR will still apply post-Brexit, but there's uncertainty around data transfer and how the ICO will participate in EU's privacy landscape
- Re-evaluate your processes, ensure you're accounting for new data uses and contracts, and pay close attention to any activities that fall within the ICO's priorities

THANK YOU!

bbcon[®] 2018

