Common Misconceptions regarding Data Privacy regulations; Mythbusters

In this article we explore the myths and misinterpretations surrounding data privacy in Europe and the UK [GDPR] and in California [CCPA]. Every individual is aware of their rights in relation to protecting their personal data. The obligations on organizations are increasingly enforceable with sanctions – monetary or reputational. This is the new business ecosystem and it is coming to a jurisdiction near you. Data as an asset is an integral part of every transaction and trade, whether local, between states or internationally. Let's focus on GDPR, in effect since May 2018 and CCPA, effective January 2020. There is much in common but the two systems do operate from different bases even while seeking to achieve the same strengthening of an individual consumer's rights and to protect those under 16.

CCPA is enforced by the California Attorney General. UK GDPR is enforced by the UK Information Commissioner. In other GDPR countries there will be an equivalent supervisory authority that monitors compliance and governance and issues sanctions.

Data privacy regulations are not new but now recognise that strengthened controls are required as data is layered onto data, data provides profiles that reach dep into our personal digital footprints and the growing discomfort that larger organizations are profiting from personal data and selling it on for gain.

Myth 1

This is all new and a burden on business.

Fact: protecting personal data has existed for a long time. What has changed is the insidious use of data captured for often different purposes and then reused in ways the individual had not expected. Codifying the respective rights and responsibilities for our digital world is new.

Action: This is all about building on your existing good practice, and what you have already done to safeguard data– in other words being smart and prepared.

Myth 2

This is all so complicated and gets in the way of day to day business priorities

Fact: this is a wakeup call that lax data handling is not acceptable anywhere, at any time. Consumer confidence in your handling of personal data is now part of customer service. Differentiate your offer by reassuring those that do business with you, that their data is safe in your hands and that it is important to you.

Action: tell your consumers what you are doing to safeguard their data and open up a dialogue so they can see you mean well and have security embedded across your operation.

Myth 3

This is a low priority and we can get around to this when we need to.

Fact: False economy. This is your organization's reputation on the line. Faced with a choice of an open, transparent statement of what you do with data, or a suspicion that information is being sold or misused without permission, where would you choose to do business?

Action: GDPR requires every organization, however small, to have a clear public statement, a privacy notice, about what they collect and how they manage the data they hold. A business that complies with GDPR and is subject to CCPA may have additional obligations under CCPA in the detail. CCPA also requires companies to disclose specific business practices in a comprehensive privacy policy. Many California companies that operate commercial websites and online services must already post a privacy policy under the California Online Privacy Protection Policy [CalOPPA]. CCPA is a natural extension to this.

Myth 4

I am small player in this field and there are more important things for me to do. This is for the big users of data that make the headlines to get their act together.

Fact: Why would you not try to meet your obligations? Under CCPA, organizations that violate the law have the "right to cure", meaning that they can change or improve any violating policies after they have been challenged. Under GDPR, similarly the regulators are also clear that the longer-term aim is to encourage good practice and ensure that efforts to meet the new requirements are recognised even if some do not meet the relevant standards. Therefore a clear intention to review and audit your processes, capture the types of data you are holding and why, is the first stage to compliant behaviour and respect for the data you are holding.

Action; Do you have a documented plan in place to regularize your data handling? If not why not? Gone are the days when marketing departments were judged by the size of their mailing list. Now it is the penetration and response rates. How many mailing lists are not compliant with CCPA? Keep good records.

Myth 5

I am too small to bother with all this.

Fact: CCPA applies to businesses with a gross revenue over $25m, have more than 50,000 customers, or where annual revenue is 50% or more based on user data. GDPR's scope is broader, affecting all businesses that handle user data even small not for profit organizations.

Action: the benchmark for robust data handling is evolving. If you have customers outside the US then GDPR or similar rules will apply. It makes sense to adopt and embrace steps to demonstrate that data is held securely and managed respo0bnsibily no matter what legal framework applies. Ultimately, the consumer will decide if they trust you and your business. Trust once lost is tough to regain.

Myth 6

If my customers opt out of the sale of their personal data, then my business will fail.

Fact: It is the "sale" of the data that is relevant here. Without confidence that you are taking your data responsibilities seriously then you will lose customers. CCPA provides explicit "opt out" options for

users who do not want their personal data sold. Organizations must include a clear link in a conspicuous place on their website that allows them to register that they do not want you to sell their data. Where consent is relied upon, GDPR operates in the same way though uGDPR, consent is not the only legal basis for use of personal data. Membership organizations will rely on the legitimate interest they have to keep track of their members, offer them services as part of their membership and manage their membership data. It seems odd that when a consumer signs up to a service that they would not want to receive updates, information about related products or simply an alert when a new service is launched. While an individual may opt out of the sale of their information, it does not mean that they opt out of you holding their data to provide services they expect.

Action: be clear about what you do with data and explain why you hold it, for what purpose and the value the consumer gets from you holding that data.

Myth 7

The rules around children do not apply to me as I clearly state that I do not have customers who are children.

Fact: Without some form of age verification or testing how would you know? You cannot avoid your obligations by putting your head in the sand. CCPA requires a positive opt-in for children under the age of 16 to consent to sale of their data. The CCPA requires businesses obtain consent from parents of children ages 13 and under, while children older than 13 can provide their own consent. Under GDPR, parents must provide consent for the processing of data of children under the age of 16.

Action: Under GDPR those handling children's personal data are required to look at a formal assessment of their processing of the data to identify risk. There are calls for a specific child safety assessment for data rather than this falling under a one size fits all standard data protection impact assessment. As we have seen from Myth 3 you are in control here to put across your business values and approach. You are in the business of instilling confidence that you handle data well and responsibly.

Myth 8

I do not keep full records so cannot provide data on request or track data breaches

Fact: Under CCPA consumers can request a copy of their data by sending "a verifiable consumer request" to an organization. There is 45 days from receipt to comply with a request. In some cases, companies can extend the time period to a maximum of 90 days. Requests under GDPR operate similarly. "Subject Access Requests" must be responded to without delay and within a month.

Action: Prepare for requests. Know how to recognise a request and when the right to know applies. Have a policy or process for how to record requests and track time limits. Unlike GDPR where access to all data held is required, under CCPA, consumers can make a request for information twice a year, and only for the last 12 months. Companies may face fines of $2,500 to $7,500 for every violation if it is deemed intentional. However, the CCPA also grants businesses a 30-day period to address a violation after receipt of a consumer's request.

Myth 9

A data breach happens rarely, and we have never had one that caused problems.

Fact: A breach can be accidental, a loss or malicious. You hold the data, so you are responsible. Under CCPA, California residents have the right to bring legal action for statutory damages if the consumer's information is subject to certain data breaches. **If** the information "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This matches the GDPR definition. The much narrower definition applicable to the data breach notification law lists specific types of information that qualify as personal information, such as a first name or initial combined with social security number. Such personal information must be nonencrypted and nonredacted; this is a new requirement.

Action: Track breaches however small and use then as a training and learning experience to demonstrate that you take your obligations seriously. Real examples bring to life the risks and issues for your staff. All organizations should ensure that staff are aware of how and to whom, within the organisation, they need to report a data breach. This will ensure that the organisations can determine quickly whether the breach needs to be reported to the authorities and the data subjects affected.

Records could include:

- A description of the breach
- The consequences and any measures taken to remedy it or its effects
- The contact details of the staff members or team that dealt with the breach
- Changes to internal procedures as a result.

Myth 10

We look after data on our systems and never have any issues we are aware of.

Fact: If a breach results from poor maintenance of reasonable security procedures and practices that would be expected then you risk that data. Breaches cost both in reputation and financially. Under GDPR, data breaches attract significant penalties: up to €10,000,000 (US $ 11.5 MILLION) or up to 2% of the previous year's total worldwide annual turnover of the organisation, whichever is higher.

Action: ensure that all data risks are assessed and documented together with all actions and processes that mitigate that risk. Lax handling of personal data is unacceptable when straightforward staff training, basic security rules around access or passwords can be set up. All organizations should have policies in place to assess risk and to be able to demonstrate compliance as a minimum. The Trust Bridge has developed a 9 step approach:

1. Review of the incident
2. Identification of the Parties involved
3. Incident Reporting
4. Data Protection Risk Analysis

5. Incident Analysis and Indicators of Compromise
6. Areas of Concern
7. Risk Mitigation
8. Improvement Plan and Lessons learnt
9. Evidence Documentation