



Primarily we at Securys think that privacy is about trust. It's no accident that we interchangeably use "confidence" to mean both trust and secrecy, we must trust in those in whom we confide.

Good privacy lies in winning and keeping that trust. The eight principles of the GDPR are merely signposts to some of the behaviours that achieve that goal; treating privacy regulation as an exercise in compliance box-ticking, while it might mechanically produce some of the outcomes intended by the legislation, will not bring with it the deeper bond that inspires confidence.

Trust is an interesting concept. It is bilateral but can be initiated unilaterally – if I demonstrate that I trust you, you will be more inclined to trust me. It is emotional but can be both supported and destroyed by cold evidence. It is fragile – how often have we seen reputations undone by a single poor decision? – but also resilient, because

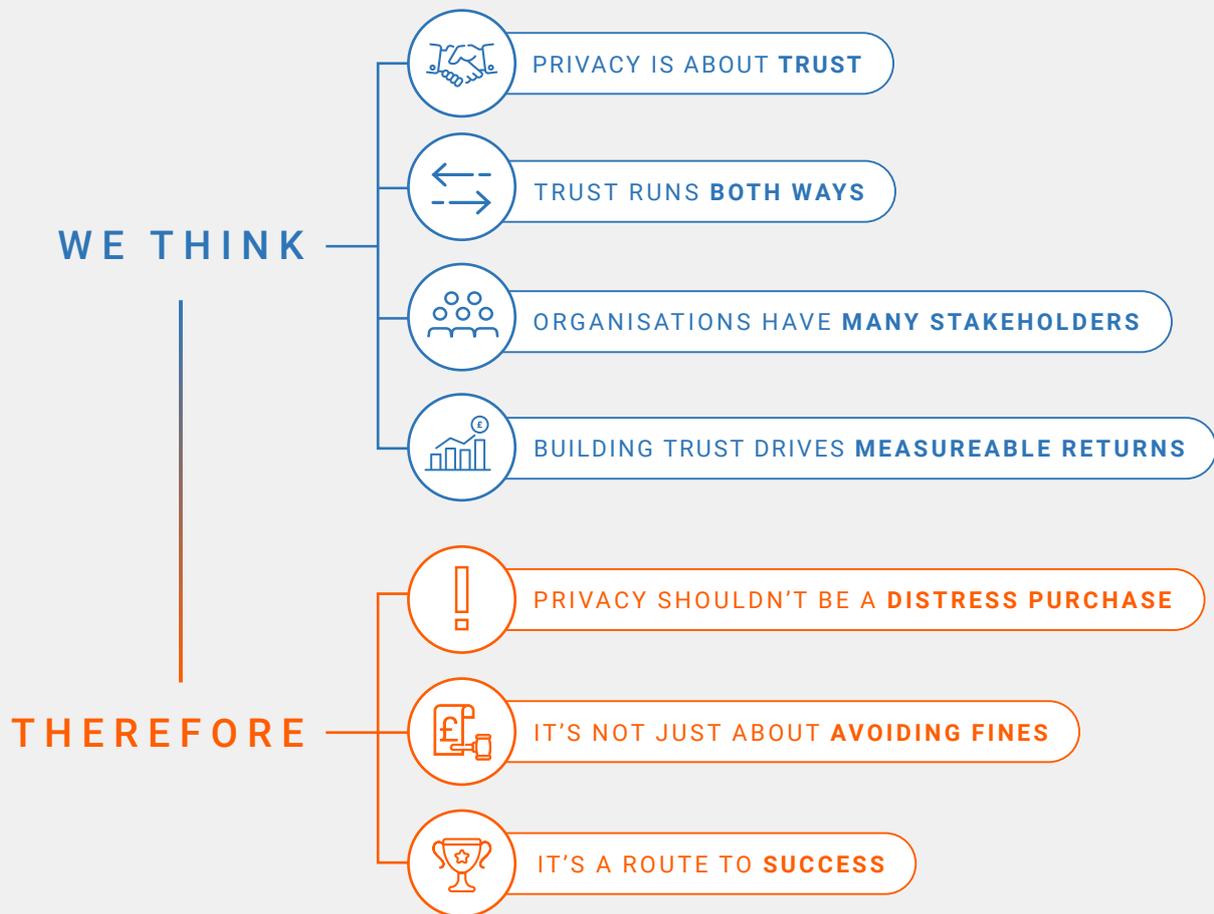
often what is trusted is the intention more than the act, so that a heartfelt apology can often compensate even for an egregious mistake. Trust is the rock on which brands are built and, like brand-building, trust is earned through consistent and repeated application of effort.

Data subjects, so people, are not stupid. They can tell the difference between an organisation that's doing the minimum to avoid regulatory sanction and one that genuinely cares about them.

—
People can tell the difference between an organisation that's doing the minimum to avoid regulatory sanction and one that genuinely cares about them.



Trust is the rock on which brands are built.



Employees will seek out, work harder for, and stay for longer with an employer who demonstrates not only that it takes good care of the data it necessarily collects about them but also that it has faith in them. Monitoring an employee's every working moment may seem like a route to enhanced productivity, but it is far from a demonstration of trust.

Consumers likewise are more likely to buy from businesses that visibly appreciate the exchange of value that is taking place – sometimes money but always data from the consumer, goods or services from the company – and that also show they likewise appreciate the responsibility placed on them as custodians of the customers' data. There is a broader element of signalling here – if a business is prepared secretly to exploit and profit from its customers' data, what other corners might it be cutting, and in what other ways might it be placing its own interests ahead of theirs?

The second decade of the 21st century has seen a strong movement amongst investors to direct funds to so-called ethical investments, often referred to as "ESG" investing, for Environmental, Social and Governance.

While it may seem easy to dismiss this as virtue-signalling, in fact it turns out that companies recognised by others as being more ethical have also historically been more successful both in financial performance and in terms of share price.

'Virtue signalling' is a pejorative term for the expression of a moral viewpoint with the intent of communicating good character.



Employees will seek out, work harder for, and stay for longer with an employer who demonstrates not only that it takes good care of the data it necessarily collects about them but also that it has faith in them.

Ultimately privacy is a part of ethics, and ethics are what lie at the heart of society. We want to live, transact, and share with people who subscribe to our idea of what “good” means, and we want to see their understanding of our common moral code throughout their behaviour – in their dealings with us personally, with other stakeholders and with society and the planet as a whole. This recognition that society is about collaboration based on trust and shared values is why ethical companies do better, and why good privacy is one step on the road to success.

It is one thing to believe that following good privacy practices delivers quantifiable benefits to business: it is another to prove it and hence be able to assert that people and companies should invest time and money in it.

Find out more

To find out more about how concerns about data privacy directly affect people’s actions and choices, and how those actions and choices feed through to your bottom line, read our specially-commissioned survey **Privacy Made Positive™** by either contacting Stuart Richards at info@securys.co.uk or by downloading the eBooks here **Privacy Made Positive from Securys**.

About Securys

Securys is a specialist data privacy consultancy with a difference. We’re not a law firm, but we employ lawyers. We’re not a cybersecurity business but our staff qualifications include CISSP and CISA. We’re not selling a one-size-fits-all tech product, but we’ve built proprietary tools and techniques that work with the class-leading GRC products to simplify and streamline the hardest tasks in assuring privacy.

We’re corporate members of the IAPP, and all our consultants are required to obtain one or more IAPP certifications. We’re ISO 27001-certified and have a comprehensive set of policies and frameworks to help our clients achieve and maintain certification. Above all our relentless focus is on practical operational delivery of effective data privacy for all your stakeholders.

