While it can be easy to think of compliance as a dry, inanimate process, we underestimate the importance of the human touch at our peril.

**While RegTech is crucial, it can’t and won’t succeed in the absence of human intuition, insight and expertise.**

The first article in this series touched on the notion that, in creating a cohesive, truly modern data privacy strategy, technology isn’t enough.

What did we mean by that, though? Specifically, what else is required?

Well, a great many things. For the most part, however, they can be crystallized into a single word, or more accurately, a single idea: trust. The creation and retention of trust.

And there is a more pressing need for it than many businesses probably realize.

In one recent study from IBM, just 20% of USA consumers surveyed said that they “completely trust” organizations when it comes to matters of data protection and privacy.
Now stop and read that statistic one more time and think about it for a moment. It’s bad enough at first glance, but on reflection it’s positively damning, right? The importance of trust can’t and shouldn’t be overestimated, despite what the “post-truth” apologists might have us believe. Trust isn’t just some spurious, soft, unimportant, politically-correct anachronism. It remains vital across a whole range of tangible, business-critical criteria.

In unlocking the benefits of data analytics, for instance. In winning and retaining customers, and fostering closer, more engaged relationships with them. In CSR, in brand, in reputation. In other words, trust has never been more essential to the business metrics that matter most of all – top line, bottom line, share price.

But why? Thinking objectively is both prudent and necessary, sure. But putting the right processes, technologies and physical checks and balances in place? Absolutely. Problems arise, however, when trust is considered only in objective terms.

Here’s the thing: in its purest form, trust is NOT objective, but intrinsically subjective. Human. Instinctive. It therefore often hinges on intangibles like emotions, personal interaction and rapport.

Accordingly, while objective, operational and technological measures are of course vital, they will very likely struggle and possibly even fail if they are not complemented, supplemented and augmented by subjective “human” measures.

The right philosophies, the right cultures, the right attitudes and behaviors. And, most crucially of all, the right people and expertise.

An organization is its people. This alone suggests that data privacy policies and procedures have to be people-centric. With around 60% of data breaches attributed to human error (therefore avoidable), the necessity becomes even clearer.

Industries that handle high volumes of sensitive data on a daily basis – financial services, medical and telecoms for example – need to be particularly vigilant and diligent. This means keeping abreast of their own industry-specific guidelines as well as broader legislation.

The question is how?

Commercial trust is, quite justifiably, born of a whole range of objective factors – transparency, accountability, governance – and, ironically, it is here that many strategies begin to go awry.

It’s clear that now more than ever, brands need to ensure that their customers know, understand and trust what data is being collected about them, how it is being used, how much of it is being shared, with whom and to what purpose.
What, then, are the kinds of people, measures and expertise firms need to put in place to start building and nurturing trust? Here are a few good places to begin:

**C-level leadership**
An executive (the role of chief privacy officer is an increasingly common one) supported by a select cross-disciplinary team – legal specialists, technologists, people and culture-leaders, and entrepreneurs – provides advice to the CPO and to the rest of the senior leadership team.

**Legal counsel**
A fully-informed, up-to-date understanding of the scope and impact of legislation across the organization and how best to strategize for it. This is best developed via the retention of expert legal counsel.

**A privacy champion**
Find advantage in appointing a privacy champion with the authority and responsibility for keeping abreast of legislative trends, changes, and solutions to keep the business compliant.

Oversee education and the instillation of data privacy as a core business value. Help prevent eleventh-hour and miscommunication emergencies, wherein the legal department has done its job but perhaps sales, marketing or engineering didn't get the message. Or abide by it.

**Trusted partners**
Privacy laws, their nuances and the constant changes to them can be extremely challenging to navigate alone.

Consulting an expert partner who knows both the legal and technological territory will ease the pressure on internal teams.

**Cultural and line-of-business leaders**
Every organization has its peculiarities. As do the lines of business and subcultures within it. It’s therefore prudent to engage with and use the expertise of those who know and understand those idiosyncrasies best: their leaders.

**Suitably comprehensive training**
It is also vital to ensure both new recruits and existing headcount are fully appraised of the importance of privacy legislation, the potential impacts of breaching it and how to remain compliant with it. It is worth considering adding privacy awareness criteria to role specifications during the hiring process, too.
The point is recognizing that the trust/privacy axis is not the domain of a single person or even a single department, but of the entire organization. It ingrains a deep, institutionalized awareness and commitment to privacy and trust. To take compliance beyond a tick-box process (something else we touched on in the first piece in this series) and make it a commercial differentiator.

**While essential, technology alone is not enough. Because while technology and automation can certainly help in ensuring trust, they can’t create or replicate it.**

For that, organizations need the right people to lead and guide them. The right experience, knowledge and understanding. Only then can they hope to forge and shape the RegTech strategies that drive not merely compliance, but genuine competitive advantage.

Businesses that embrace such an approach will see their brands thrive in the next commercial age – one in which trust will be not less important, but more and more critically so. Those who don’t? Let’s just say they’ll struggle.

To learn more about Hitachi’s specialist Digital Privacy expertise and solutions visit our [site](#)