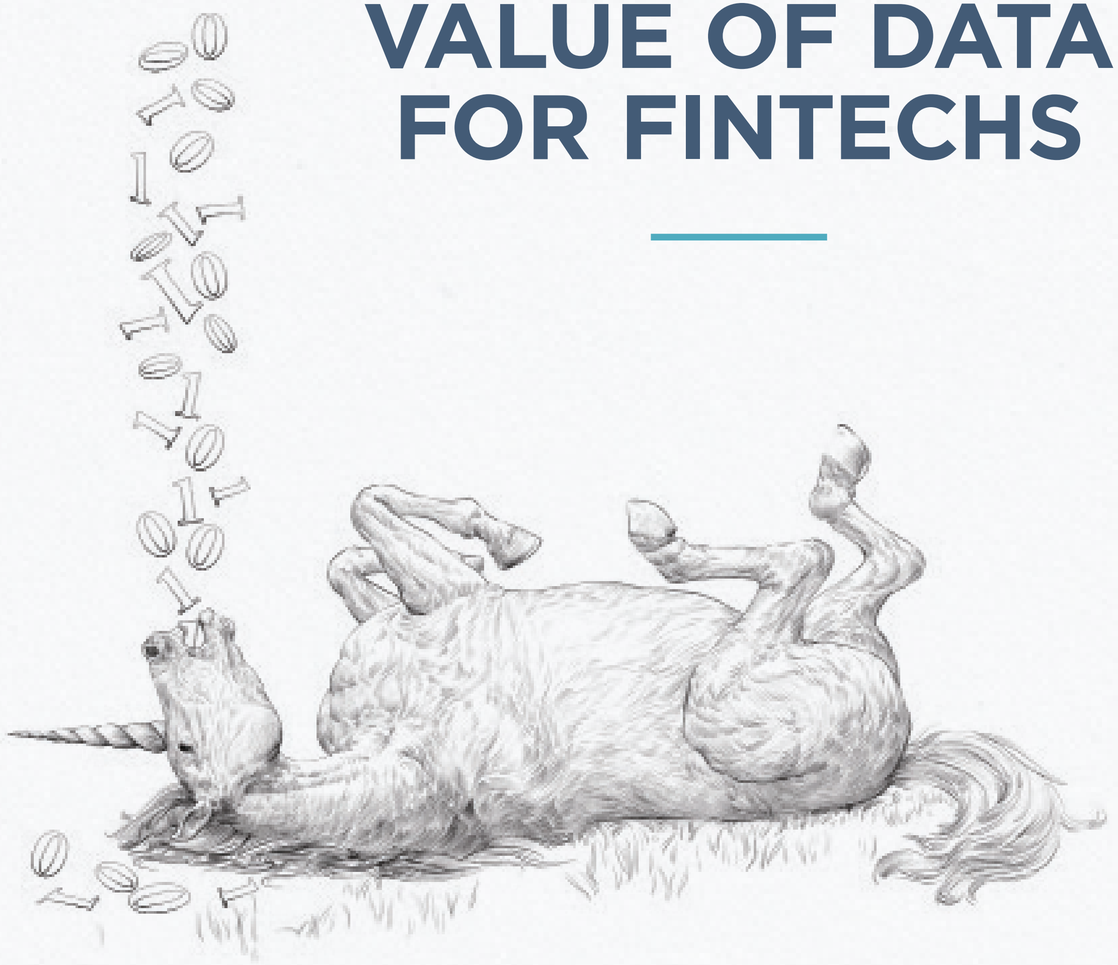
DATA AND PRIVACY

UNLOCKING THE VALUE OF DATA FOR FINTECHS



Tapping into the personal data you hold and enabling your clients to do so is key to staying competitive.

Often unquantifiable, yet always immense, fintechs unlocking this value through the use of advanced analytics techniques, such as machine learning, are uncovering patterns that can inform their business decisions, improve customer experiences, unlock new revenue streams and drive growth.

Creating the ability to target customers more effectively, provide customised investment advice, create increasingly personalised loan offers and build more accurate credit scoring models to assess the risk of lending, successfully leveraged personal data can create competitive advantage and increase customer engagement.

However, the ability to tailor products and services to meet the specific needs of customers does not come without risk. The collection, processing and sharing of personal data is highly regulated, and any non-compliance will likely lead to heavy penalties both financially and reputationally. By extension, even the most compliant fintech firm is vulnerable to the risk of data breaches through penetration of systems, often involving sensitive information.

Despite being under increased pressure to use smart solutions to tap into the value of the data you hold, you should remain alert to these risks:

i. always collect high-quality data;

ii. be transparent about what you are doing;

iii. implement secure storage and processing systems; and

iv. build a data-driven culture within your fintech firm.

DATA FUNDAMENTALS OF DATA COMPLIANCE FOR FINTECH

1. COMMUNICATE CLEARLY

Transparency is key: Customers, users and clients must be aware of what you are doing with their data. This includes how personal data is collected, used and shared.

You must provide a privacy notice stating clearly what you do with personal data, where you get it from and where it ends up:

i. for any profiling this means letting people know clearly the consequences of the profiling; and

ii. if it looks creepy when you write it down, you probably shouldn't be doing it!

2. SECURE THINKING

Create a safe haven! Think about the technical and organisational measures you use to protect personal data. Are these appropriate for your processing activities?

Enhance your protection by, for example:

i. encrypting personal data;

ii. utilising strong access controls;

iii. implementing firewalls & intrusion detection systems; and

iv. ensuring that employees are trained on data protection and privacy practices....

and remember it's not just about IT – collaborative working spaces are great for young companies, but you need to be aware of practical challenges to security when loading sensitive information on screen or discussing it in these spaces.

3. CONTINUOUS ASSESSMENT

Review, review, review... For bigger projects you will need to do a data protection impact assessment, but things move quickly on fintech development projects and your privacy compliance must be reviewed regularly. This is relevant throughout a project lifecycle:

i. ***at the start of a project*** - conduct risk assessments to identify potential weaknesses in data protection;

ii. ***during the project*** – review contractual arrangements with, for example, hird party partners processing personal data on your behalf to ensure they meet these requirements; and,

iii. ***at all stages*** – ensure that security measures remain robust.

4. INCIDENTS DON'T JUST HAPEN TO OTHER PEOPLE: PLAN AHEAD

Remain penalty proof: Everyone is vulnerable to a breach, even with rigorous security. Regulatory penalties and claims generally only happen to organisations that are not prepared well enough to respond.

To avoid penalties for non-compliance, implement an incident response plan that is easily accessible, fast-moving and concise.

Bring in the right expert teams at the start and make sure they are briefed in the event of an incident. Expose employees to mock breach incidents and be aware and ready to submit a regulatory notice if needed, within 72 hours of becoming aware of a breach.

DON’T LET DATA SCUPPER YOR DEAL!

1. DILIGENCE

i. Check that you have permission to use your datasets!
ii. What are your lawful bases?

2. CONTRACTS

i. Do these give you all necessary rights to the data set?
ii. Can you comply with all data protection obligations?

3. SUPPLIERS

i. Are any suppliers high-risk (outside of the UK or Europe)?
ii. Do you have sufficient assurances from them?

4. HIGH RISK DATA

i. Are you doing anything with high-risk data (e.g. medical, biometric, financial)?
ii. Identify and minimise the data protection risks through your impact assessment!