

360Science Thought Leadership Series

The 1-10 -100 – 10,000 Rule [updated for GDPR]

It's like Moore's Law...

If you're not familiar with the 1-10-100 rule — it's a quality management concept used to quantify the hidden costs of poor quality. **Think of it as Moore's Law applied to data quality.**

Dr. George Labovitz and Yu Sang Chang developed the rule in 1992, **to underscore that failure costs are significantly greater than prevention costs.** But now in 2018, with new government regulations like the EU's GDPR and California's Consumer Privacy Act CCPA that goes into effect on January 2020 - Labovitz and Chang's rule is out of date, and out of touch with the new realities of data regulation and compliance.

These new laws contain broad sweeping definitions of personal information. As you would expect, personal information includes data points like people's names, email addresses, geolocation data, and Social Security numbers. It also covers other personally identifiable information (or 'PII'), such as: IP addresses, shopping, browsing and search histories; and consumer profiles that are derived based on inferences from personal information.

Compliance is mind boggling complex, and the fines imposed by these laws are jaw-dropping.

GENERAL DATA
PROTECTION REGULATION

If someone covered under GDPR wants a company to delete his or her data, send copies of the data, or correct an error in the data, companies must comply.

The 1-10 -100 – 10,000 Rule [updated for GDPR]

THE COST OF COMPLIANCE

NEW 10,000X: Compliance/Legal Cost

The cost when data processes lead to critical breakdowns, and the financial strain brought on by the compliance issue. Costs involved include the fines mandated by the regulation, but also correcting the issue, labor, legal, and ongoing oversight, along with damage to market reputation and share value.

100X: Failure Cost

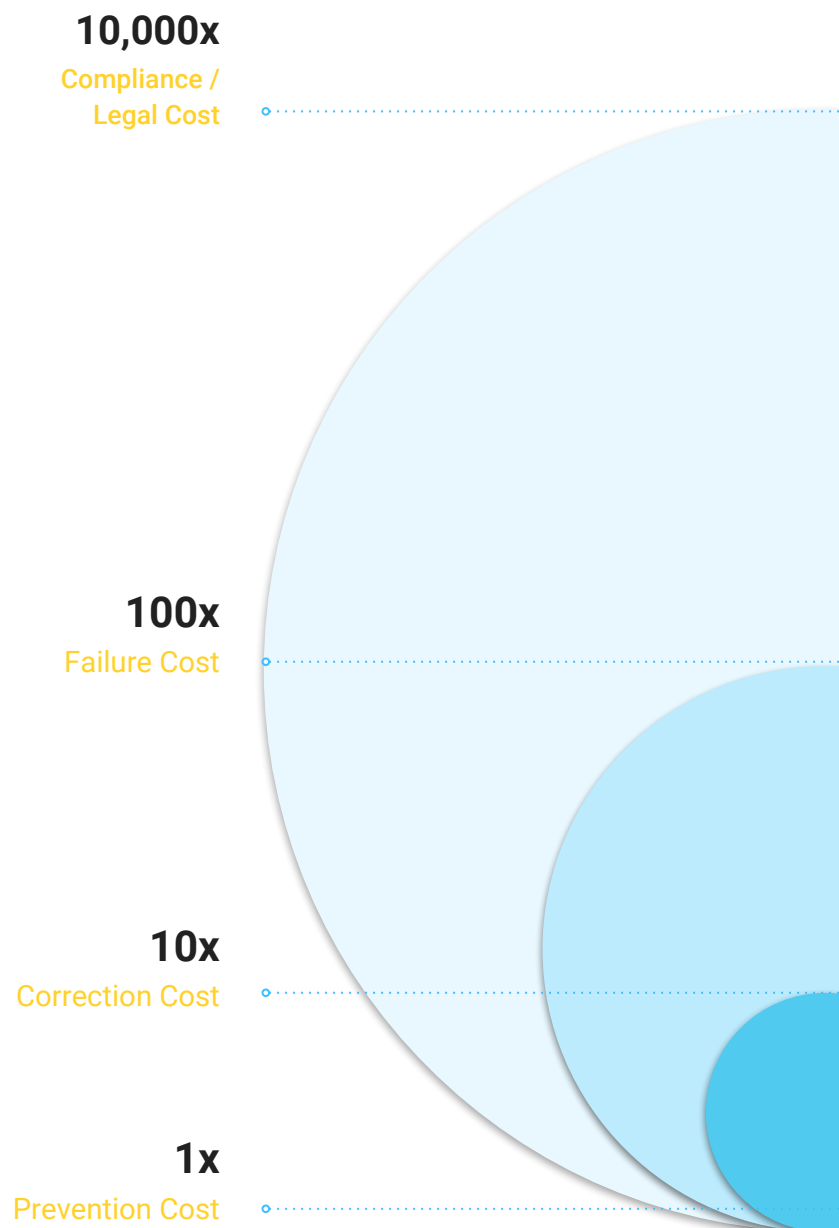
The cost if nothing is done at all, and using poor/outdated data in business operations and in data analysis.

10X: Correction Cost

When prevention stage is skipped, cost to correct a record – scrubbing, de-duping, matching, and verification.

1X: Prevention Cost

The cost of verifying data quality at the point of creation.



Breaking Down GDPR

What is GDPR, and why was it enacted?

The General Data Protection Regulation is a sweeping law that gives residents of the European Union more control over their personal data and seeks to clarify rules and responsibilities. It replaces the EU's previous law governing data protection passed in 1995 and strengthens the data rights of EU residents.

Why was it enacted? The short answer is because of public concern over privacy. In general, Europe has had more stringent rules around how companies use the personal data of its citizens, and with GDPR it harmonizes data protection laws across all EU member states.

Which companies does GDPR affect?

The GDPR applies to any organization that handles the Personally Identifiable Information (PII) of EU residents.

Companies do not have to be based in the EU to be bound by GDPR. They only need to be processing or holding data on EU residents in order for GDPR to apply to them. This includes most major online services and businesses that collect, process, manage or store data (data handlers).

There are two different types of data-handlers the legislation applies to: 'processors' and 'controllers'. The definitions of each are laid out in [Article 4 of the General Data Protection Regulation](#).



Individuals covered under GDPR can now object to specific ways companies use their data and can tell a company to stop using their information for a particular purpose.

What kind of data does the GDPR protect?

- Basic identity information such as name, address and ID numbers
- Web data such as location, IP address, cookie data and RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

GDPR expands on what companies must consider as personal data. The regulation requires companies to closely track the data that they store. If a person wants a company to delete his or her data, correct errors in the data, or send copies of the data the company has on them - companies must comply.

If that's not onerous enough, the law goes even further than that. Individuals covered under GDPR can now object to specific ways companies use their data and can tell a company to stop using their information for a particular purpose.

What are the penalties?

Under GDPR, organizations in breach can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). In California, the CCPA imposes penalties of \$750 per consumer per incident (e.g., \$750,000 for an incident involving a database file of just 1,000 consumers).



On 25th May 2018... the maximum fine for breach of data protection regulations increased from €500,000 to €10 million or 2% of global gross revenue (whichever is higher).

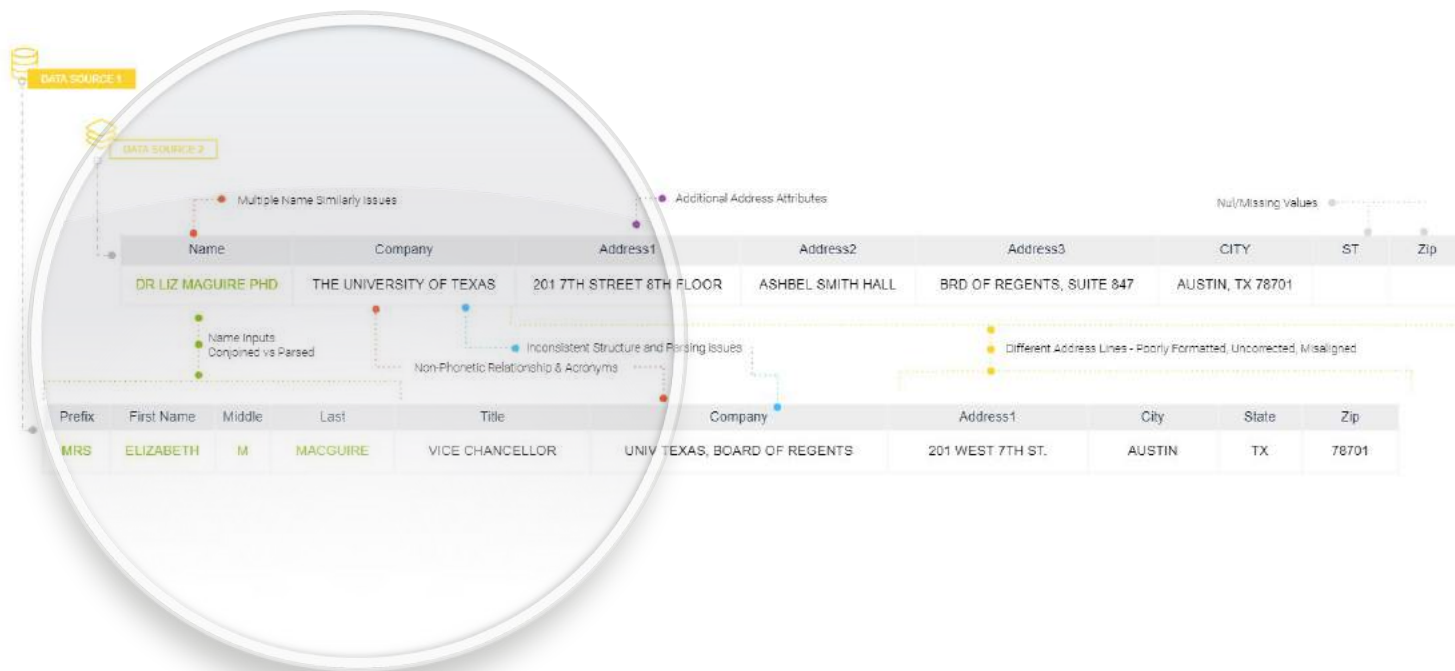
That's just for a lower level breach, these amounts double for a level 2 breach!

Conclusion

Today — Customer data matching is going require more than a toolbox of regular expressions

Customer data unification has never been just an IT problem – it’s a business problem, and the impact is measurable in terms like CAC, LTV, CRR, AAGR, CAGR, and Loyalty. With GDPR enacted it’s now squarely a shareholder issue and the 1-10-100-10,000 rule applies.

According to a [2018 RSA Data Privacy & Security Report](#) - The lack of trust in how companies treat their personal information has led some consumers to take their own PII data security countermeasures. According to the RSA report, **“41 percent of the respondents said they intentionally falsify data when signing up for services online.”** Conventional data matching processes that rely on impossibly clean, extracted, parsed, transformed, normalized, standardized, and enriched data - will only further struggle to cope with matching this data.



The fact is - no one ALGORITHM, METHODOLOGY, or MATCHCODE can be relied on exclusively to deal with all variations found in a typical database. **That’s why we created 360Science!**

The AI Matching Engine Built for Customer Data Applications

Agile & Accessible



We believe customer data unification should be easy regardless of a user's technical ability. 360Science simplifies every step of the process.

Seriously Powerful



Deterministic and probabilistic logic combine with artificial intelligence to deliver as much as 226% more accurate match rate on CRM customer.

Enterprise Ready



360Science offers world-class APIs and toolkits - as well as pre-built integrations for many data analytics and data integration platforms!



Get in touch!



3001 S Lamar Blvd #101
Austin, TX 78704
866.332.7132



www.360science.com
hello@360science.com
@360ScienceHQ

