evident proof

DIGITAL DATA EVIDENCE 100% VERIFIABLE

NALYTICS®
search rediscovered

Case study

Prove the power of your data and Reduce your risk

Delivering Immutable, Unhackable data verification, provenance and data proof services

Regulatory & Compliance

NALYTICS®
search rediscovered

Business Problem – SARS, GDPR Data Redaction

Organisations struggle to respond to Subject Access Requests in the time allowed and typically do not have a defined SAR processes in place. They need a way to prove they have complied with GDPR.

Currently companies have to search their data for relevant information, which can be spread across multiple data sources.
They need to prove that they have excluded exempt data such as legally privileged information, management information, opinions or confidential references. Ensuring only the relevant information is returned for review.

Goals

1. **Business Requirements:** Tracking SARS Data procedure removal and workflow process
2. **Required Outcome:** Legally verifiable proof that they have Excluded exempt data that should not be disseminated, such as sensitive, confidential , or third party information and confirmation that the SAR redaction has taken place
3. **Key Commercial ROI:** Safety for the public, Mitigate risks, Cost Reduction, Reduction of Financial liability

evident proof
DIGITAL DATA EVIDENCE 100% VERIFIABLE

Background

Core Industry Problem

Under GDPR, individuals have the right of access to any personal information and data related to them that is held and processed by an organisation and request the information is redacted.

Costs

For example: local government bodies average cost of a SAR/Redaction is £1,400 Local government bodies averages 138 SARs per year.
There are 418 local government bodies. Estimated annual cost of around £90 million

The average cost of a SAR across the public sector was £1400

NALYTICS®
search rediscovered

Understanding the SARs process and the response output required to meet legal requirements:-

- Time limitations GDPR requires organisations to respond to a SAR within one month i.e. 30 days of its receipt. You must get back to the individual with the requested information without undue delay.
- Exempt data needs to be excluded such as legally privileged information, management information, opinions or confidential references
- Censor data to obscure details that should not be disseminated, such as sensitive, confidential , or third party information. Redact within the Nalytics viewer or from a copy of the original source document.

Solution

The Evident Proof Solution has provided the Nalytics with the tools to generate reports called Proof Certificates that verify the workflow order correctness, completeness and the time-order of its submitted digital records.

How does this work?

Data from the SARS request procedure is connected to the Evident Proof platform, its unique systems encrypts the data, timestamps it and stores it securely on the blockchain.

These encrypted pieces of data are added to an unchangeable chain of blocks in chronological order. Once added it is not possible for data to be altered, deleted, or tampered with

Business Outcome ROI

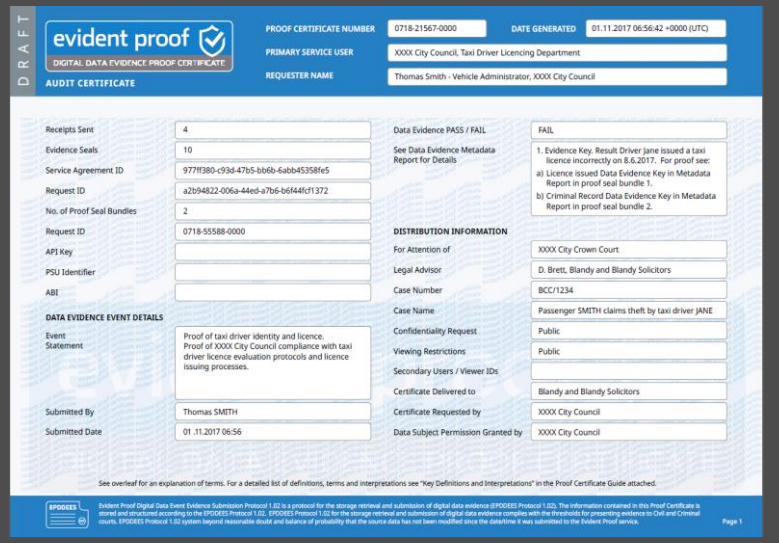
- ✓ Nalytics can verify to all clients their data collection & workflow activities
- ✓ Thanks to the Evident proof protocol this data is now legally verifiable confirming the correct checks have been carried in accordance with the Law.
- ✓ Nalytics and its client has reduced risk as it can mitigate any legal claims
- ✓ Full accountability is now in place with a transparent auditable trail
- ✓ Costs are reduced – All data that is required for legal verification can be pulled together quickly from a single source of truth.

NALYTICS®
search rediscovered

Evident Proof enables our clients to reduce their risk
Nalytics helps organisations prepare their Subject Access Request responses in an easier, faster and more cost effective way

Evident Proof provides irrevocable proof of the data & workflow that has taken place to exclude and censor personal data during the redaction process.

Mac Exon-Taylor
Nalytics


DRAFT

evident proof
DIGITAL DATA EVIDENCE PROOF CERTIFICATE

AUDIT CERTIFICATE

PROOF CERTIFICATE NUMBER 0718-21567-0000
DATE GENERATED 01.11.2017 06:56:42 +0000 (UTC)
PRIMARY SERVICE USER XXXX City Council, Taxi Driver Licencing Department
REQUESTER NAME Thomas Smith - Vehicle Administrator, XXXX City Council

Receipts Sent	4
Evidence Seals	10
Service Agreement ID	977ff380-c93d-47b5-bb6b-6abb45358fe5
Request ID	a2b94822-006a-44ed-a7b6-b6f44fcf1372
No. of Proof Seal Bundles	2
Request ID	0718-55588-0000
API Key	
PSU Identifier	
ABI	

DATA EVIDENCE EVENT DETAILS

Event Statement	Proof of taxi driver identity and licence. Proof of XXXX City Council compliance with taxi driver licence evaluation protocols and licence issuing processes.
Submitted By	Thomas SMITH
Submitted Date	01.11.2017 06:56

Data Evidence PASS / FAIL	FAIL
See Data Evidence Metadata Report for Details	1. Evidence Key. Result Driver Jane issued a taxi licence incorrectly on 8.6.2017. For proof see: a) Licence issued Data Evidence Key in Metadata Report in proof seal bundle 1. b) Criminal Record Data Evidence Key in Metadata Report in proof seal bundle 2.

DISTRIBUTION INFORMATION

For Attention of	XXXX City Crown Court
Legal Advisor	D. Brett, Blandy and Blandy Solicitors
Case Number	BCC/1234
Case Name	Passenger SMITH claims theft by taxi driver JANE
Confidentiality Request	Public
Viewing Restrictions	Public
Secondary Users / Viewer IDs	
Certificate Delivered to	Blandy and Blandy Solicitors
Certificate Requested by	XXXX City Council
Data Subject Permission Granted by	XXXX City Council

See overleaf for an explanation of terms. For a detailed list of definitions, terms and interpretations see "Key Definitions and Interpretations" in the Proof Certificate Guide attached.

EPODEES

Evident Proof Digital Data Event Evidence Submission Protocol 1.02 is a protocol for the storage retrieval and submission of digital data evidence (EPODEES Protocol 1.02). The information contained in this Proof Certificate is stored and structured according to the EPODEES Protocol 1.02. EPODEES Protocol 1.02 for the storage retrieval and submission of digital data evidence complies with the thresholds for presenting evidence to Civil and Criminal courts. EPODEES Protocol 1.02 system beyond reasonable doubt and balance of probability that the source data has not been modified since the date/time it was submitted to the Evident Proof service.

Page 1

About Evident Proof

Evident Proof Transform's data, documents, transactions and workflows into tamper proof, unchangeable records

Evident Proof runs alongside existing database activities and workflows, No need to change existing databases or code.

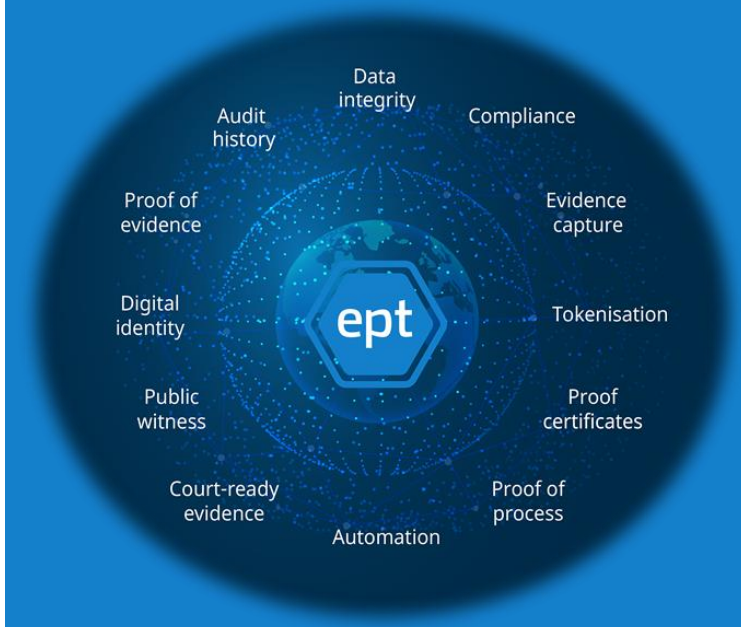
- ✓ **Non disruptive technology**. It's quick to set up using NuGet and Visual Studio plugins
- ✓ In just 7 mins, the Evident platform can be plugged in to run alongside **any of your datasets.**

Evident Proof stores proof seals of **any type of data**, document, transaction and even entire workflows onto an immutable and un-hackable blockchain

- ✓ At the press of a button **any data or workflow** activity can be output as a Proof Certificate
- ✓ Evident Proof Certificates are **100% irrefutable evidence**, applicable in UK & European Civil and Criminal Courts and tribunals
- ✓ The platform enables you to protect your data from any threat and saves organisations **£1000's in legal fees**, and data fines

evident proof

DIGITAL DATA EVIDENCE 100% VERIFIABLE



Contact us

Data Proof Operations EP Ltd
enquiries@evident-proof.com
Phone: +44 (0) 118 380 5520
Website: Evident-proof.com