GENERAL DATA PROTECTION REGULATION STATEMENT FOR CUSTOMERS

Document Version: 1.2 **Date last reviewed:** 04 August 2017
Document Owner: Tracy McAvoy **Review date:** 08 January 2018

Overview

Destin Solutions is a processor of data, receiving data from third party Data Controllers (customers who we process data on behalf off) these include Local Authorities and Debt Collection agencies. Data is also taken from Credit Reference agencies (CRA's) and other organisations (e.g. Land Registry) who specialise in the provision of data. Destin Solutions does not engage with nor collect data directly from data subjects.

Destin Solutions deal solely with data processing in the UK, all data received and processed is information based on and collected from UK citizens only. Data is not transferred internationally nor hosted or shared outside the confines of the UK.

Destin Solutions agree that Personal data will be processed on behalf of customers lawfully, fairly, and in a transparent manner in relation to the data subject. At all times, we will only process data on behalf of our customers, the Data Controllers.

Data Processed

Destin Solutions processes data on behalf of customers in a number of different areas. Types of data processed include property information, citizen information and local business information. A list of typical attributes in the datasets processed can be found in Appendix 1 at the end of this document.

Data Recipients

The recipients of this data are the customers previously mentioned i.e. UK-based Local Authorities and Debt Collection Agencies. This data is securely held and processed using methods outlined in related policy documents (Information Security Policy and Guidelines for Processing of Personal Data for Customers) and is not shared with any other third parties.

Purpose of Data Processing by Solution Type

VISION and Fusion

VISION and Fusion are two solutions provided by Destin Solutions to customers. Both solutions collate data on individuals and companies for the purpose of ensuring the appropriate level of tax and liability is paid to those customers. This is a legislative requirement and both solutions enable the aggregation, filtering and matching of data sets across different systems. These systems typically include Revenues, Housing, Sundry Debtors, Parking and Benefits systems.

VISION as a tool is responsible for segmenting data, effectively slicing and dicing the data in different ways to provide customers with deep insights into the data they hold. It does not make assumptions about the data held.

For example it will take citizen data and match this to data provided by the customer on balances, transactions and collections to ascertain whether a citizen is in debt to the Council.

Fusion however does make assumptions about data held, using fuzzy matching. Fuzzy matching is used to help match records which are in fact of the same object but have been recorded differently, for example due to miss-spelling.

For example three sets of data may exist across three different systems as follows;

- Joe Blogs aged 45 lives at 65 Blackton Avenue, Richland, TK10 7UX
- Joe Bloggs aged 45 lives at 63 Blackton Avenue, Richland TK10 7UX
- Joel Bloggs aged 45 lives at 65 Blackton Avenue, Richland, TK10 7UX

When using Fuzzy matching to try and cleanse and ensure accuracy of data held, the consolidated result this would return would be;

- Joe Bloggs aged 45 lives at 65 Blackton Avenue, Richland, TK10 7UX

It matches the 1st record and the 3rd record as high probability and wouldn't automatically match the middle record as it can determine it has a lower probability of being the same record.

The Fuzzy algorithms used are proprietary as is the way in which they are used for matching. When a record has been Fuzzy matched, it is marked and a link to the full record can be provided, ensuring there is a full audit trail. Users also have the option to either confirm or reject the fuzzy match.

The application of the Fusion solution to our Customers data helps meet GDPR requirements around ensuring data is kept accurate and up to date.

Sensitive personal data (i.e. sexual life, political opinions, religious beliefs, physical/mental health, trade union membership, alleged/actual criminal record) is not processed by either solution. Ethnicity however is processed by our solutions as it is captured by Data Controllers who provide us with this data in the first instance but data can be redacted so that it is made unviewable when linking data sets together.

The processing of data by these solutions enables Local Authorities and Debt Collection agencies operating on behalf of Local Authorities, to develop and refine an effective debt recovery strategy in line with associated policies (e.g. urban renewal, vulnerable groups, discounts and exemptions). It also ensures customers can monitor processes and staff activities to improve efficiency and effectiveness in delivering core strategy.

The processing of data using these solutions also helps customers combat fraud and tax evasion by identifying potential instances of false claims in order to receive certain discounts, exemptions and benefits which in fact the subject may not be entitled to.

The solutions are an essential tool in ensuring that customers have on hand all the relevant information they need to deal with individual cases and that data held on subjects across different systems are both consistent and accurate.

Ascendant

Ascendant is a solution which takes data from a number of different, external non-local authority sources such as credit reference agencies and land registry and matches this data to specific Local Authority data to create a single view of their citizens and businesses. This consolidated dataset is all held and viewed within a secure web portal and enables customers to make more informed decisions.

Data is processed in this way to enable a number of applications as follows;

Single person discount (SPD) reviews – existing council data can be taken and cross referenced against a series of credit referencing data and other external checks to identify instances of fraud, error or misrepresentation in SPD claims.

Empty homes reviews - takes a council's empty properties list and checks it against a series of external sources including land registry and property and rental agreements to identify up to date contact information on owners and renters. Access to this information ensures appropriate tax exemptions, reliefs and discounts can be reviewed for accuracy.

Business rates reviews - provides ongoing analysis of local businesses and commercial entities and the Directors associated with them to identify their health, wealth and trading status. The service enables Councils to keep on top of business rates collections and proactively tackle instances of fraud and growing debt.

Council Tax – appends existing council data to make sure the most up to date contact information is held on citizens and can help trace individuals who may have left properties with no forwarding details, so that debt can be recovered expediently.

Aspire

Aspire is a solution provided by Destin Solutions to customers which enables them to take any process that is documented and administered from within a spreadsheet or similar software package and automates it using a web based portal. Its purpose is to help Local Authorities, cut down on repetitive, labour intensive, manual tasks.

Aspire takes data from staff caseloads to help track cases, prompt staff when follow up action is required and routes cases at key points in a process. It can provide detailed analysis and reporting on each stage within a process and this can be cross referenced against employee tasks, outputs and productivity.

Aspire assists in tracking the individual performance of an employee within the organisation and to assess how they are performing against key targets, goals and work contracts. Customers should be aware that making use of this functionality is likely to constitute monitoring of employees and they are responsible for ensuring that this is carried out transparently and fairly.

Actions taken to ensure personal data is accurate and kept up to date

As outlined at the start of this document Destin Solutions does not directly collect data from subjects, this is the responsibility of the Data Controller (our Customers and other third parties) who supply us with this data to process in the first instance. It is therefore the responsibility of the Data

Controller to ensure personal data initially provided to Destin Solutions for processing is accurate at the point of collection.

However as highlighted earlier in this document, the Fusion solution provided by Destin Solutions views information taken from multiple different systems and through Fuzzy matching ensures data is appropriately cleansed, keeping it up to date and accurate on an ongoing basis.

Measures taken to protect data

Destin Solutions have created numerous documentation highlighting the measures we take to protect customer data under the new GDPR. In particular against unauthorised or unlawful processing of personal data, accidental loss or destruction of, or damage to personal data. It is also worth noting that customer data is all securely partitioned off, so each individual customer only has access to their own citizens relevant personal data.

Destin Solutions policy documents are available on request and include;

- Information Security Policy – outlines how we establish and maintain the security/confidentiality of information, information systems, applications and networks owned by Destin Solutions.
- Removable Media Policy - establishes the principles/working practices that are to be adopted by all users on the rare occasions where data may be required to be safely stored and transferred on removable media.
- User Access Management Policy – highlights the precautions taken to prevent unauthorised access to our information systems and includes details on password policies and privilege management.
- Teleworking Policy – sets out the high-level principles and expectations we have of staff who are remotely working.
- Incident Management Process Flow – provides an overview of the steps taken in the event of an incident, including how these are identified, logged, categorised, prioritised, diagnosed and closed.
- Breach Notification Form – outlines breach details in the event of an incident, and covers containment/recovery, assessment of ongoing risk, notification of breaches, evaluation and response.
- Guidelines for Processing of Personal Data for Customers – covers points on the recruitment of employees and contractors, physical security, business continuity.
- Disaster Recovery Plan – covering processes and timescales involved in getting systems back up and running in the event of a major incident, incorporating target recovery points and target recovery objectives

Security Controls employed

Identity and Authentication

Accounts given to staff only have access to the minimum information and resources that are necessary for their job role. Members of staff which from time-time need to perform operations with elevated permissions will be provided with one or more elevated accounts to be used only when necessary to perform those tasks.

High privilege accounts must only be used when accounts of lower rights will not perform the tasks required.

Log management software is used to audit access to critical systems and detect inappropriate

or suspicious access-related events including use of high privilege accounts.

User authentication and management access authentication both use 2-factor authentication.

Asset Protection

All data is stored and processed in UK data centers which comply with industry standards. All physical media is encrypted, protecting data at rest. All penetration testing is currently conducted inhouse and carried out at least once per year.

Security Governance

Ultimate responsibility for information security rests with the Managing Director of Destin Solutions, but on a day-to-day basis the Data Security Manager is responsible for implementing the policy and related procedures.

Line Managers are responsible for ensuring that their permanent/ temporary staff and contractors are aware of:-
- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

Line managers are individually responsible for the security of their physical environments where information is processed or stored. Each staff member is responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall ensure the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Contracts with external contractors allowing access to the organisation's information systems are in operation before access is allowed. These contracts ensure that staff or sub-contractors of the external organisation comply with all appropriate security policies.

Operational Security

Our networks are protected by Intrusion Protection Systems (IPS) to identify, block and log the following common network attacks:

- Ping of Death
- IP half scan
- Port Scan
- Ping of Death
- Land
- DNS attacks

Our IPS is configured to scan and drop IP packets that contain IP options that are indicative of

suspicious and potentially malicious behaviour.

We use Dell Intrust log management software which enables real-time notification of critical events through email alerts and automatic responses to certain events such as disabling a user account. Response times depend on priority level.

We use an incident management process flow chart. Users report incidents by phone, email or the portal interface. Incidents are then identified, logged, categorised and prioritised. Following incident diagnosis and resolution incidents are closed subject to users agreeing to the closure. Incidents are fully documented and an incident record is kept. Incident reports are available to customers whom have been impacted by the incident on request, via email.

People Focussed Controls

During recruitment, references are obtained and checks made that these and the candidate's qualifications are valid. The employment contract explicitly states that employees can only process personal data with a valid contract with a customer. During employee orientation, each new employee receives proper training on the importance of confidentiality of covered data and information and on proper use of computer information and passwords.

Regular information security and data protection training is provided for all staff and the release of any new company documentation in this area is reviewed, shared and presented, so that staff are fully informed of our current policies in this area.

Security Check and Audits

We are currently in the process of working towards our ISO 27001 accreditation and expect to achieve certification by December 2017, with a preliminary audit conducted in November 2017. As and when penetration tests and information security audits are conducted we are happy to provide summary results of theses in order for Customer to assess our security and carry out due diligence.

Meeting General Data Protection Regulation Obligations

Destin Solutions have taken the time to review the specific text of the GDPR and confirm that we agree to act on the instructions of Data Controllers (i.e customers) and mirror the obligations Controllers themselves have on Security and Employees. Furthermore we agree not to disclose any data without the consent of our customers or unless there is a duty to disclose imposed by law or the requirements of a regulatory body but only to the extent so required.

Data breaches and audits

If we become aware of any personal data breaches without undue delay we will alert the Data Controller. Where applicable Destin Solutions shall maintain a record of data processing activities under its responsibility, for each customer. This will be achieved using management information captured within our solutions providing a full audit trail to highlight where data has been supplemented, appended and effectively processed.

Customers have access to real-time audit information within our applications.

Children and vulnerable adults

At present none of the Destin Solutions offerings, process any data specifically relating to children or vulnerable adults.

Automation and decision-making

All of the solutions offered by Destin Solutions provide a level of automation, for example taking multiple records of similar information and merging it automatically into one 'best match' record. This does not impact on any kind of decision making process in our opinion but if required, functionality can be added in to facilitate human intervention before the final merge occurs so that records can be manually agreed or approved.

Time limits for erasure

All of the solutions offered by Destin Solutions require ongoing processing of data on a daily basis because data such as work tasks, collection balances, recovery action and transactions are continually being updated. On this basis, data storage and processing will occur for the lifetime of any contract agreed. It is worth noting however, the accuracy and matching processes described earlier in the document help to ensure that individual citizen records which are no longer current or relevant to the Clients' purposes are deleted from the system at the earliest opportunity.

Upon the ending of any contract Destin Solutions agree to securely remove data provided by Data Controllers from its systems within 7 days.

Profiling

All of the solutions offered by Destin Solutions come with profiling functionality in order to derive information on future trends and patterns that may help improve future decision making. For example is council tax recovery slower in one district compared to another? Typically the profiling carried out is not done at an individual level, it is based on grouped information of multiple records. A more detailed example might be where reports from the solution are run to identify whether council tax collections are slower in a particular region, among a particular age group, which might indicate a more proactive approach needs to be taken to collections. In this example although the process of collecting and gathering that data is automated, the reports enable customers to rapidly analyse the data themselves before any final decisions are made. The customers will make decisions based on both the data returned alongside the experience they have accumulated over the years rather than delegating it to an automated process. Essentially the profiling capabilities of the technology facilitate decisions being made by experienced people who have the right information in front of them at the time.

Destin Solutions can confirm that it uses appropriate mathematical or statistical procedures for any profiling functionality conducted. It has implemented appropriate technical and organisational measures to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, as per Article 71 in the GDPR.

Data Protection Officer

Destin Solutions agree to appoint a Data Protection Officer (DPO) to ensure ongoing compliance with the GDPR and who can fulfil the tasks as outlined in Article 39 of the GDPR. These tasks include;

- to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation;
- to monitor compliance with this Regulation, including the assignment of responsibilities, awareness raising and training of staff involved in the processing operations, and the related audits;

- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- to cooperate with the supervisory authority (the ICO);
- to act as the contact point for the supervisory authority on issues related to the processing of personal data

The DPO will maintain a current record of all the clients (data controllers) for whom we are processing data, and the type of processing carried out on their behalf, in compliance with Art 30 (2) of GDPR.

This document will be updated with the contact details of the DPO as soon as they are appointed and those contact details will be provided to customers.

Identification of risk related to Data Processing

As outlined in Article 75 of the GDPR we have reviewed the likelihood of risk to the rights and freedoms of natural persons resulting from the data processed on behalf of our customers. Accordingly we have outlined in the table below, the risk level and how Destin Solutions intend to mitigate against these risks.

Risk Type	Risk Level	Mitigation
Discrimination	Low	As the majority of sensitive information is not processed by Destin Solutions, this minimises any chance of discrimination. In the case of ethnicity data this information can be redacted / made unviewable during data processing, ensuring no decisions or outputs can occur based on a subjects ethnicity.
Identity theft / fraud, financial loss	Low	Banking information relating to data subjects is not processed by our solutions, minimising any chance of financial loss. We safeguard against identity theft and fraud by adhering stringently to the guidelines outlined in our Information Security Policy, which is available upon request.
Reputation damage	Low	All data is held and processed securely and in line with the procedures and responsibilities as outlined in our Information Security Policy.
Loss of confidentiality of personal data protected by professional secrecy	Low	All data is held and processed securely and in line with the procedures and responsibilities as outlined in our Information Security Policy.
Unauthorised reversal of pseudonymisation	Low	Reversal of pseudonymisation can only be authorised by a user with

		the appropriate privileges and access rights to the system. These rights are allocated on the authority of company Directors who manage this process in accordance with our User Access Management Policy.
Individuals deprived of rights and freedoms, or prevented from exercising control over their data	Low	We have in place a process which enables us to securely create a readable file in a recognised format, containing all data held on an individual, following verification of the identity of the individual.
Processing sensitive data, including data on racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership; genetic data; health data; data concerning sex life; or data on criminal convictions and offences or related security measures	Medium	The only sensitive data we currently process is based on ethnicity and this information can be redacted and made unviewable when looking at individual data subject records.
Profiling (personal aspects are evaluated [e.g. analyse or predict work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements] to create or use personal profiles)	Medium	Profiling of information related to citizens will be conducted at a high level and reports returned to experienced individuals who will analyse the data before making any decisions that may have a detrimental effect on subjects.
Processing children's and vulnerable persons' data	Low	No data relating to children or vulnerable people is currently processed.
Processing large amounts of data affecting large numbers of individuals	Low	The data we process is limited to tax payments, benefits, discounts and exemptions received as well as employee productivity. All data is held and processed securely and in line with the procedures and responsibilities as outlined in our Information Security Policy.
Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data	Low	Measures we take to safeguard against this are outlined in our 'Guidelines to the Processing of Personal Data for Customers' document, which is available upon request.

Conclusion

This document is fluid and will be updated over the coming year to reflect changes made to better meet the needs of the GDPR coming into force in May 2018. Destin Solutions is committed to

monitoring the latest developments and guidelines issued by supervisory bodies in the UK to ensure our role as a data processor meets the standards legally required.

A copy of the latest version of this statement has been made available on our website and a link to it can be found at the bottom of the following page http://www.destin.co.uk/privacy/

This document has been independently reviewed by Act Now Training – www.actnow.org.uk.

Appendix 1

List of Data processed on behalf of customers

Property
UPRN (Unique property reference number as allocated by land registry)
PropertyNumber
StreetName
PostCode
PostTown
PostSector
Area
PostCodeArea
longitude
latitude
DataPoint

CitizenToCitizen
ChildCitizenKey (number allocated to an individual but doesn't exist outside the datawarehouse)
ParentCitizenKey (number allocated to an individual but doesn't exist outside the datawarehouse)
Relationship (e.g landlord, employer, brother)
StartDate
EndDate

CitizenToProperty
CitizenKey (number allocated to an individual but doesn't exist outside the datawarehouse)
Relationship (e.g. owner, tenant)
StartDate
EndDate

CitizenToAccount
AccountType
AccountName
StartDate
EndDate

Citizen
CitizenID
Gender
DateOfBirth
Ethnicity
Title
ForeName
SurName
NationalInsuranceNumber
MaritalStatus

Businesses
COMPANY_NUMBER
COMPANY
PNR
ADDRESS1
ADDRESS2

ADDRESS3
ADDRESS4
POST_CODE
DATE_OF_APPOINTMENT
COMPANY_NAME
COMPANY_REG
COMPANY_ADDRESS1
COMPANY_ADDRESS2
COMPANY_ADDRESS3
COMPANY_ADDRESS4
COMPANY_POST_CODE
WEBSITE
TELEPHONE
TPS_FLAG
SIC_CODE07
SIC_DESCRIPTION
CREDIT_RATING
RATING_DATE
CREDIT_LIMIT
FAX_NUMBER
INCORPORATION_DATE
TRADING_OFFICE_ADDRESS1
TRADING_OFFICE_ADDRESS2
TRADING_OFFICE_ADDRESS3
TRADING_OFFICE_ADDRESS4
TRADING_ADDRESS_POST_CODE
ANNUAL_ACCOUNTS_DATE
TURNOVER
PRE_TAX_PROFIT
NET_WORTH
NUMBER_OF_EMPLOYEES
AUDITORS
DC_YEARS_TRADING
DC_NUM_EMPLOYEES
DC_LTD_NONLTD_FLAG
DC_INCORP_DATE
DC_FAX
DC_URL
DC_IS_ACTIVE
DC_CONTACT_TITLE
DC_CONTACT_FIRSTNAME
DC_CONTACT_SURNAME
DC_CONTACT_DOB
DC_CONTACT_OCCUPATION
DC_NATIONALITY
DC_MULTIPLE_DIRECTORS
DC_ULT_PARENT_BIN
DC_ULT_PARENT_NAME
DC_PARENT_BIN
DC_PARENT_NAME
DC_CREDIT_RATING
DC_CREDIT_LIMIT
DC_PREV_CREDIT_RATING
DC_RATING_DATE
DC_LIMIT_DATE
DC_INTERNATIONAL_SCORE
DC_EQUITY_IN_PERCENT
DC_CREDITOR_DAYS
DC_LIQUID_ACID_TEST
DC_RET_CAP_EMP_PERCENT
DC_RET_TOTAL_ASSETS_EMP_PERCENT
DC_CURRENT_DEBT_RATIO_PERCENT
DC_TOTAL_DEBT_RATIO_PERCENT
DC_STOCK_TURNOVER_RATIO_PERCENT
DC_RET_NET_ASSETS_EMP_PERCENT
DC_CURRENT_RATIO
DC_SALES_NET_WORKING_CAPITAL
DC_GEARING_RATIO_PERCENT
DC_CCJ_COUNTS
DC_CCJ_VALUE
DC_SHAREHOLDERS
DC_PRINCIPLE_ACTIVITY
DC_NET_CASHFLOW_OPS
DC_NET_CASHFLOW_BEFORE_FIN
DC_NET_CASHFLOW_FROM_FIN
DC_CONTINGENT_LIABILITY
DC_CAPITAL_EMPLOYED
DC_AUDITORS
DC_AUDITORS_QUAL
DC_BANKERS
DC_MTG_OUTSTANDING
DC_MTG_OUTSTANDING_TIMESTAMP
DC_MTG_SATISFIED
DC_MTG_SATISFIED_TIMESTAMP
DC_MTG_PARTIAL
DC_MTG_PARTIAL_TIMESTAMP
DC_TANGIBLE_ASSETS
DC_INTANGIBLE_ASSETS
DC_TOTAL_FIXED_ASSETS
DC_TOTAL_CURRENT_ASSETS
DC_TRADE_DEBTORS
DC_STOCKS
DC_CASH
DC_OTHER_CURRENT_ASSETS
DC_MISC_CURRENT_ASSETS
DC_TOTAL_ASSETS
DC_TOTAL_CURRENT_LIABILITIES
DC_TRADE_CREDITORS
DC_BANK_OVERDRAFT
DC_OTH_SHORT_TERM_FIN
DC_MISV_CURRENT_LIABILITES
DC_OTH_LONG_TERM_FINANCE

DC_TOTAL_LONG_TERM_LIABILITIES
DC_TOTAL_OVERDRAFT_LTL
DC_TOTAL_LIABILITIES
DC_NET_ASSETS
DC_WORKING_CAPITAL
DC_PAID_UP_CAPITAL
DC_PROFIT_LOSS_ACT_RESERVE
DC_SUNDRY_RESERVES
DC_REEVAL_RESERVES
DC_SHAREHOLDERS_FUNDS
DC_NET_WORTH
DC_ACCOUNTS_TO_FROM
DC_MONTHS
DC_CURRENCY
DC_CONSOLIDATED_ACCOUNTS
DC_TURNOVER
DC_EXPORTS
DC_COST_OF_SALES
DC_GROSS_PROFIT
DC_WAGES_SALARIES
DC_DIRECTORS_EMOLUMENTS
DC_OPERATING_PROFIT
DC_DEPRECIATION
DC_AUDIT_FEES
DC_INTEREST_PAYMENTS
DC_PRETAX_PROFIT
DC_TAX
DC_DIVIDENDS_PAYABLE
DC_RETAINED_PROFITS
DC_PRETAX_MARGIN
DC_POSTTAX_PROFIT
OccupancyStatus
Occupier
JointName
NameInAddress
Deceased
DeceasedConfidence
DateOfSale
SalePrice
PropertyType
Tenure
AveDetachedPropValue
AveSemiDetachedPropValue
AveTerracedPropValue
AveFlatPropValue
TelephoneNo
ExDir
P2PScore
DOB
BAIOrderType
BAIRestrictionType
BAIOrderStatus
BAIOrderNumber
BAIOrderDate
BAICourt
JudgementActiveCount
JudgementTotalAmount
LatestJudgementStatus
LatestJudgementDate
LatestJudgementAmount
NumberOfPortfolios
AccountType
DOBMatch
DOBMultipleMatches
InputDOB
Distance
Cohabiting (true or false)
JobNo
DateRun
TTF_URN
TTF_Email
TTF_EmploymentStatus
TTF_LandLine
TTF_MobilePhone
TTF_Occupation
TTF_DateLastActiveAtAddress
JobReference
RunDate
RowURN
RowImportDate
fkClientID