Forensic Analytics

Digital Forensic Experts

Forensic Analytics

The Forensic Science Regulator's Code of Practice 2023:

What does regulation of working with communications and cell site data mean for me and my organisation?

THE QUEEN'S AWARDS FOR ENTERPRISE: INNOVATION 2021

Contents

Introduction

In a positive development for policing and criminal justice, the Forensic Science Regulators' Statutory Code of Practice new code of conduct was approved by both houses of Parliament in February and March and will now come into force on the 2nd of October 2023. The code sets quality standard requirements for Forensic Science Activities (FSAs') related to the investigation of crime and the criminal justice system in England and Wales.

The code includes standards of conduct and practice for a number of FSAs' that fall under the definition of Digital Forensic Science Activities. One of these activities is that of Cell Site Analysis for Geolocation (FSA – DIG 200 – Cell site analysis for geolocation). At Forensic Analytics, we have been following the development of the code of practice closely and welcome the rigour with which deals with this particularly important activity.

As expected, we have been receiving a great many enquiries from the UK Law Enforcement community about the new code and what it means for the full range of practitioners involved in the use of communications data in the course of their work: Investigators, Analysts, RF Technicians and Expert Witnesses, and other Forensics Practitioners. This position paper has been written to address those questions. It explains what the Cell site section of the code regulates and what it does not, who it affects, when it comes into effect & when compliance is required by, and what needs to be done to achieve compliance.

The reassuring news for all concerned is that regulation is welcome, and a positive step forward. Secondly, it is reasonable and measured, and will serve only to empower the users of this data, who have in fact been working in a proto-compliant environment for many years. Thirdly, the timeline for compliance is reasonable, and allows for enough time for all forces, agencies, and organisations to perform careful gap analyses and work to finalise any adjustments without impeding ongoing operational activity, or adversely affecting existing workflows.

The new code of practice, and the value it brings.

The new code is a consequence of the Forensic Science Regulator Act 2021, which places the Regulator on a statutory basis as a new legal entity and provides the Regulator with legal powers. The code comes into force on 2 October 2023, and for those organisations who undertake work covered by “FSA – DIG 200 – Cell site analysis for geolocation” there is a 24-month period from that date to achieve compliance.

Regulation, when done right, is a force for good, for all professionals and organisations that it affects. Responsible and diligent professionals welcome good regulation, as it allows well-run teams and departments to thrive and succeed in their role, giving a clear framework to operate within, and enables them to produce material that can be understood by others as being of a standard and of objectively measurable quality that gives the end user confidence in its utility and relevance to them.

Forensic science is an important component of criminal investigations; contributing to the identification of offenders and to the evidential material presented in the courtroom. The Forensic Science Regulator correctly points out that it is one of the strongest safeguards against false allegation and wrongful conviction.

At the heart of good regulation is the intention to reduce error and risk. Forensic science work carries significant risks, and quality failures can have serious consequences. Where failures are individual, rectification can be complex and challenging. Where failures are systemic, the consequences can be organisation wide, expensive, and reputationally catastrophic. Any opportunity to minimise the chances of that should be welcomed. Correctly generated evidential product also makes for a much more level playing field in the courtroom, with clarity prevailing over ambiguity. The new code of practice is intended to ensure that accurate and reliable scientific evidence is produced, and to minimise the risk of quality failures, miscarriages of justice and failed prosecutions.

Where legitimate systems and processes are already in place in an organisation, new regulation should serve to support and encourage further development of those already exceptional working practices; it should not impede or prevent people from doing good work where they had been before. The good news is that the new Code of Practice is a model of well drafted guidance: it is not too prescriptive or bureaucratic; it is proportionate and timely, thorough, and fair.

The key elements of quality management addressed in the code are; the validation of methods; competence of personnel; documented, controlled and auditable procedures; commitment from senior leadership; enabling of continual improvement.

In the next section we will address the parts of the code that relate to the Forensic Science Activity that is of greatest relevance to customers of Forensic Analytics: FSA DIG 200: Cell Site Analysis for Geolocation.

FSA DIG 200: Cell site analysis for Geolocation.

What is regulated?

The Forensic Science Activity "FSA – DIG 200 – Cell site analysis for geolocation" is the component of the code that states minimum standards for the processing of communications data (CDRs), the publishing of data schedules, the publishing of maps based on that data, radio frequency surveying, and the giving of expert opinion the communications data and radio frequency outputs. All organisations undertaking this FSA will be required to achieve compliance and accreditation to the code and ISO/IEC17025:2017.

What is exempt?

Section 97 "FSA – DIG 101 – Analysis of communications network data" provides exemptions from compliance with the code, and states that when the following activities are carried out for the purpose of informing the investigation where products such as maps and charts are clearly marked as "This forensic information is not intended as evidence," these activities are not covered by the Code.

a) Processing and normalisation of CDR or other network provider data for the purposes of informing the investigation.
b) Relational or temporal analysis of CDR information.
c) Presumptive automated tools for analysing CDRs, including 'co-location' analysis, and accepting the risks and limitations, including confirmation bias.
d) Production of mapping of cell sites and/or cell site coverage for informing the investigation.

Who does it affect?

The code effectively delineates three categories of practitioner:

1. Those who work with communications data and whose work is not intended to be used as evidence. These may be investigators, analysts, or other professionals whose work is only used to inform investigations or intelligence operations. These practitioners are exempt from the code as per the definition within Section 97 "FSA – DIG 101 – Analysis of communications network data".
2. Those who work with communications data and who only ever produce outputs such as charts, tables and maps that may be used in evidence, and whose work simply represents the raw data. These may be investigators analysts or other professionals who provide communications data evidence or appear in court as witnesses of fact. The work of these practitioners is regulated by the code.
3. Those who work with communications data and who may perform all the functions listed above, plus any of: RF surveying, cell site analysis, or the application of their expert opinion to conclusions drawn on that work. These would be professionals who act as expert witnesses in their provision of evidential output or their appearances in court. The work of these practitioners is regulated by the code.

When does it come into effect?

The code comes into effect on 2 October 2023. Compliance with the code is required within 24 months of that date, i.e. 2 October 2025. That leaves more than two years for all organisations affected to work towards compliance.

What needs to be done to achieve compliance?

Broadly speaking, the work required to demonstrate an organisation's compliance with the cell site sections of the code can be broadly placed into three categories: Systems/Processes, Validation and Competence.

It is important to note that many organisations within law enforcement already hold a significant amount of UKAS accreditation to ISO17020, ISO17025 and the current version of the Forensic Science Regulators Code of Practice for a wide range of forensic disciplines. This gives significant reason for optimism as organisations already operate policies, processes, procedures and comprehensive quality management systems which will provide all with a stable platform to progress an extension to scope for "FSA – DIG 200 – Cell site analysis for geolocation"

The below provide Forensic Analytics initial insight into the three broad categories listed:

Systems/Processes:

Organisations who carry out cell site work should review their existing Standard Operating Procedures (SOPs) that relate to commissioning, strategy, methodology, checking and review, and validation of work. Forensic Analytics have been consulting widely in the UK Law Enforcement arena on this subject for many years and can state with confidence that in a great many cases SOPs are already in place. There is certainly work to be done, but the timeline allows for a methodical approach. We recommend a three-stage process:

1. Careful review and undertake a gap analysis of your existing SOPs seeking to understand which staff ought to be affected by those SOPs, where are the gaps in the content or in the application of the SOPs across the organisation.
2. Update documentation considering the gap analysis, control the SOPs in the Quality Management System and inform all affected parties. The group of affected parties may well include several practitioners who previously had not been affected by them.
3. Implementation organisation-wide, with dedicated project management and linkage to existing Quality Management Systems.

Validation:

All technical methods used in "FSA – DIG 200 – Cell site analysis for geolocation" are required to be fit for purpose; this can be demonstrated by method validation against requirements of the end user which will be defined by the validating organisation. The methods can be defined as those activities that are undertaken with regard to the FSA i.e. undertaking of a Radio Frequency Propagation Survey using LIMA Cell Monitor, cell site analysis using CSAS and provision of associated evidential reports / statements.

This involves establishing that the method operates in a manner that fulfils the acceptance criteria derived from the end-user requirements, that the limitations of the method are properly understood, that the planned use of the method is appropriate, and that the approach to reporting is logical.

Undertaking validation of a method allows a proper understanding of the risks involved in its use.

Forensic Analytics are progressing full validation pertaining to "FSA – DIG 200 – Cell site analysis for geolocation" and have applied to UKAS with regard to applying for accreditation to ISO17025 and the Code of Practice for the use of LIMA Cell Monitor and CSAS (version 3) for Cell Site Analysis. Our aim upon achievement of this accreditation and overall code compliance is to be able to provide relevant support to our customers as appropriate as each progresses its own activity for validation / verification for this FSA.

An immediate element of assurance is IntaForensics successfully validating and achieving accreditation for our LIMA Cell Monitor and CSAS capability to ISO17025 and the non-statutory version of the Forensic Regulators Code of Practice.

Competence:

There is a requirement for each organisation / unit undertaking "FSA – DIG 200 – Cell site analysis for geolocation" to determine and document the requirements for competence and ongoing competence for each role undertaking the FSA including the competencies required for reporting findings.

A competence framework for practitioners involved in this FSA should include the following:

a. education;

b. qualification;

c. training, including statement/report writing and courtroom skills;

d. technical knowledge;

e. skills and experience;

f. the nature of the competence assessment;

g. the frequency of reassessment of competence; and

h. whether observation of any testing or examinations are required, and if so, the frequency of this.

Regarding competence, your training record is your first port of call. As above and in Section 110 of the code there is clarity on the competence requirements, and staff's training histories are the bedrock on which to begin a programme of updating and adding to the evidence of their competence.

Over the last several years, Forensic Analytics have delivered training in the subject matter required by "FSA – DIG 200" to thousands of UK Law Enforcement staff, and we continue to roll that training out to practitioners. We can work with you to review the requirements of the code against your staff's competence and provide recommendations for filling any skill or knowledge gaps within the time allowed for under the code.

Note also that the code requires maintenance and regular refreshing of competence, and Forensic Analytics' training offering includes regular CPD updates for practitioners.

Conclusions:

The introduction of the statutory Forensic Science Regulator's Code of Practice marks an opportunity for those working in the field of forensics to work to a new and robust framework. This will serve to improve the professional confidence of staff and increase the credibility and professionalism of their roles. Most importantly, it serves to apply a new standard of rigour to the processes of working with forensic material, ensuring that evidential standards will remain high, and the risk of error and misinterpretation will be minimised.

In relation to FSA DIG 200, the code has now formalised the good work done and high standards already followed by thousands of practitioners in the UK on cell site and communications data. To coin a phrase, the FSR hasn't re-invented the wheel. Forensic departments have robust quality control systems, and the existing SOPs in relation to cell site work must now be reviewed and then incorporated into those quality systems.

The competence of all practitioners must be assessed, and any gaps in skills and knowledge must be filled with high quality training, externally accredited and verifiable. Practitioners must also periodically refresh and update their learning. Again, organisations across the UK have already done a lot of hard work to drive competence, and this stands them in good stead for the work to be done on achieving compliance.

While all of this this will entail careful, methodical work, your organisation is not starting from scratch, you have sufficient time to complete it without sacrificing ongoing operational capability, and we and your colleagues in the forensics sector are here to help.

Forensic Analytics Ltd April 2023

Appendix 1: FSA DIG 200: Relevant sections of the code that relate to competence.

Section 28 of the code gives a general commentary on the subject of competence. It stresses the need for relevant education and training, including in the areas of statement and report writing and courtroom skills. When it comes to technical competence, this is set out in detail under the sections that deal with each specific Forensic Science Activity, but section 28 makes sure to stress that frequency of reassessment of competence is a key requirement.

Section 83 of the code is the first main explanation of the FSA "DIG 200: Cell site analysis for geolocation". It explains at a high level which sub activities that organisations and individuals need to demonstrate competence in. Section 110 of the code takes the general outline provided in section 28, and then goes into further detail, adding specific requirements.

Combining sections 83 and 100, the code regulates the following activities and specifies the following competence requirements:

A. For practitioners involved in processing and normalisation of CDRs and creating or adopting maps of cell sites and/or cell site coverage for the purpose of reporting to court, these persons should be able to provide proof of training that covers knowledge of:

a) Relevant communications data
b) Normalisation of data;
c) quality assurance stages
d) Accepted practices for differentiating between estimated coverage plotted for planning purposes and factual plotted data.
[ref: paragraph 110.9.2]

B. For practitioners involved in RF propagation surveying, these persons shall be assessed against a range of criteria including:

a) Survey strategy
b) Survey methodology
c) Survey equipment settings
d) Limitations of survey types and data
e) Knowledge of Wi-Fi and RF communications standards
f) responsibilities of practitioners
g) Report writing
[ref: paragraph 110.9.3]

In addition to the above, there are requirements for:

C. The forensic unit to demonstrate ingoing competence of all practitioners [110.9.4]

D. Training to include the following subjects:

a) Legislation awareness [110.9.5 and 110.9.6]
b) An understanding of assessment of evaluative evidence [110.9.7]
c) Examination strategy for cell site analysis, assessment and interpretation, theory training on inference, cognitive bias and preparation of expert reports and statements [110.9.8]
d) Roles and responsibilities of an expert at court, including opinion and interpretation [110.9.9, 110.9.10 & 110.9.11]

Appendix 2: Forensic Analytics Courses that teach the competencies required by FSA DIG 200

Radio Frequency Propagation Surveys

Course code: FA312

Duration: 10 days

The timely collection of digital evidence provides the investigator and court with ground truth data. The delivery of clear, concise, and confident witness testimony in the courtroom is vitally important in the effective presentation of evidence and ensuring witness credibility.

This course has been designed to enhance practitioner understanding of Radio Frequency Propagation Surveys (RFPS) and the practical skillset to undertake surveys and present survey results. Topics include the cellular architecture, cellular and Wi-Fi generations, and the planning, deployment, and coverage objectives of mobile network operators. The course explores the principles of Radio Frequency Propagation Surveys and techniques, including the integrity of and the reliance that can be placed on the collected data. Instruction is also given on the preparation of intelligence and evidential standard RFPS reports.

A full day on the presentation of evidence in the courtroom, delivered by an experienced Barrister, will improve courtroom confidence by providing an understanding of the theory, process, and practice of delivering witness testimony with an emphasis on clear and concise presentation of evidence, and key insights into the tactics and techniques used by Defence Lawyers. The theory is supported by a series of scenario based practical exercises, which includes undertaking a survey and a courtroom roleplay relating to the presentation of evidence under examination in chief and cross examination. This course has been developed and is delivered by RFPS practitioners, with experience planning communication networks and presenting expert evidence in court.

CDR processing and interpretation

Course code FA215

Duration: 3 full days/5 half days

Accredited by City & Guilds, this course offers an externally recognised qualification in CDR cleansing, processing and analysis. It provides an in-depth exploration of how mobile networks work and how and where call data is captured. Attendees will explore the meaning and relevance of CDR fields and examine the investigative benefits that an understanding of the data can provide. Current CDR formats are examined in depth and exercises that offer hands-on practice of cleansing/parsing that data are undertaken.

Next generation comms data analysis

Course code FA217

Duration: 2 full days/4 half days

Ideal for CD analysts, this course examines new and upcoming forms of communication, network types and calling techniques: 4G, 5G, VoLTE, SRVCC, Wi-Fi Calling and VoIP, among others. It gives an overview of how these new services and technologies work and looks at the CDR data that they provide. The purpose is to prepare CD analysts for the types of data that will become common in the near future, and how to extract evidence from them.

Interpreting GPRS billing workshop

Course code FA237

Duration: 1 day

Mobile data records (known generically as “GPRS” data) are increasingly important to the Analyst and Investigator. When examined and interpreted with appropriate care and attention to detail, this information source can be a surprisingly rich source of geographic data and of certain aspects of users’ communications. Over the course of this day’s training, delegates will be shown examples of, and work with, sample data from each of the telephone service providers. Detailed explanations are given as to the methods by which phone companies provide data connections, and how the billing records are generated. By the end of the course, attendees will be able to recognise and make use of a variety of leads and investigative opportunities that routinely appear in the data.

Comms data analysis techniques

Course code FA238

Duration: 2 days

This course is designed to enhance operational analytical capabilities by providing a thorough understanding of the theory and practice of a range of analytical techniques with an emphasis on getting maximum benefit from the opportunities offered by different data formats. Instruction is given on the role and responsibilities of an Analyst within an operational environment, and on key concepts such as lifestyle analysis and the importance of attributing telephone numbers and devices. Instruction is also given on the methods of achieving attribution and the techniques used to examine geographical data to identify significant address and potential co-location between clean and dirty phones, potential meetings between associates and to identify vehicles.

Investigate with CSAS

Course code FA435

Duration: 2 days

Cell Site Analysis Suite (CSAS) cleanses, simplifies, combines, analyses and visualises complex data sets instantly, saving crucial time during investigations and providing fast access to data insights; and for those working on real-time cases, swift operational decisions can be made when time is of the essence. This course has been designed to improve operational understanding of basic communications data concepts and use of CSAS to gain investigative leads through a blended learning experience. Instruction is given on the meaning and relevance of call detail record (CDR) fields, how they can be used to interpret the data and the investigative benefits that an understanding of the data can provide. To fully convey the operational utility of CSAS, instruction is given on the main features of CSAS during three scenario-based exercises, which demonstrate how to apply and utilise the main functions of CSAS to interpret communications data to inform effective decision making and drive different types of investigations forward.

CSAS Advanced

Course code FA405

Duration: 3 days

This course is designed to enhance confidence and knowledge in the use of CSAS to an advanced level by providing a complete and detailed instruction of the deeper functionality of the software, so that it can be utilised to its fullest potential to interpret digital formats in operational environments. Instruction is given on all features and functionalities, such as the troubleshooting unrecognised digital formats, interpreting the visual parser/cleansing process, interpreting complex analytics such as the county line valuation and viewing multiple different digital formats in the advanced data browser and managing time offsets between events on handset / SIM card downloads and call detail records (CDRs). The theory is supported by exercises that offer practical experience of applying the concepts and techniques required to progress an investigation using CSAS.

Map with CSAS

Course code: FA441

Duration: 1 day

This course has been designed to improve map presentation skills by providing a thorough understanding of the theory and practice of using the CSAS mapping module to display geographic elements of an investigation with an emphasis on producing an impactful representation of the geographic evidence. Instruction is given on overlaying different sources of geographic data, the use of graphics, iconography, content, labelling and map arrangements. The theory is interweaved within a scenario-based exercise to cement the key learning points.

Forensic Analytics

Digital Forensic Experts

CSAS

CDAN
Nexus

ForensicRF
Services

Training
Services

Consultancy
Services

Forensic Analytics Ltd | Registered in England and Wales. Company No: 08606475
Pixmore Centre, Pixmore Avenue, Letchworth, SG6 1JG

+44 800 158 3830 | www.forensicanalytics.co.uk